PBX evolution Nortel is getting ready to launch the first in a family of Linux-based IP PBXs. PAGE 8.

Call 911 Emergency service needs to be seen as a requirement, not a feature, says columnist Johna Till Johnson. PAGE 35.

NetworkWorld

The leader in network knowledge ■ www.nwfusion.com

April 18, 2005 ■ Volume 22, Number 15

A Wider Net

Expanding city Wi-Fi net proves no day at the beach

Wireless plan becomes tangled in politics.

■ BY JOHN COX

You may be able to see the future of municipal wireless networks unfolding in Hermosa Beach, Calif. And it's not pretty.

The city last summer launched a public Wi-Fi network based on wireless mesh radios. The goal was to create free wireless Internet access as an alternative to broadband services offered by Adelphia, Verizon and others.

But since December, the five-person city council has been locked in increasingly rancorous debates over whether the wireless LAN (WLAN) should be expanded across this 1.3-square-mile bedroom

See Hermosa Beach, page 14

DAN VASCONCELLOS

How vulnerable is the 'Net?

Security upgrades ongoing, but some argue more needs to be done.

■ BY JIM DUFFY

The unusual activity began two weeks before the attack. Officials from the Cooperative Association for Internet Data Analysis, which had begun monitoring Internet nameserver behavior at the start of 2002, noticed varying levels of performance degradation in early October of that year. Little did they realize that on Oct. 21 they would witness a flood of ping messages on the Internet's 13 DNS root nameservers that would cause the most notorious denial-of-service attack on the Internet to this date.

■ Does a secure Internet need its own version of the Sarbanes-Oxley Act? Page 13.

"It was an attempt to make a massive problem," says KC Claffy, principal investigator at CAIDA. "They certainly made a blip on a graph."

But the Internet and its users got off easy. The barrage lasted only an hour, and no end users were affected.

The attack did, however, serve as a wake-up call, as network operators and others have taken steps to better secure the Internet since then. But some still question whether the Internet is susceptible to attack and needs more authoritative oversight.

"If somebody was to do a real concerted, knowledgeable attack, it wouldn't be very difficult to have a catastrophic impact on a huge component of commerce," says Larry Jarvis, vice president of network engineering at Fidelity Investments. "It would be huge to the U.S. economy and to a lot of companies that now view the Internet as the equivalent to a

See Vulnerable, page 12

NEWSPAPER ■ $5.00

910

AT&T pushing legacy services onto MPLS net

■ BY DENISE PAPPALARDO

AT&T is migrating a host of legacy services to its Multi-protocol Label Switching IP network with the goal of making it easier, and in some cases less expensive, for users to support audio conferencing, videoconferencing, IP Centrex and toll-free services.

The carrier is expected to announce the services in the second half of the year. The services will run over AT&T's worldwide MPLS network and primarily are aimed at current MPLS VPN customers. AT&T's MPLS network has 1,000 nodes and is available in 60 countries.

In addition, the carrier intends to extend the reach of its VoIP support to include local connectivity, says Michael Antieri, product management group executive at AT&T.

But AT&T declined to provide details such as where local VoIP would be available, whether it is teaming with other local service providers or if it's deploying gateways around the country to support local VoIP.

Industry watchers say local VoIP support will be key in extending legacy services such as audio

See AT&T, page 8

Your potential. Our passion.

Microsoft

TOYOTA

NAME

Ms. 25% Lower TCO on Dealer Infrastructure Management

"Ten percent of my IT group used to be dedicated just to monitoring our systems. Now they're dedicated to providing new services to dealers."

Mylene Mayers
Technology Manager, *Toyota Motor Sales USA*

Make a name for yourself with Windows Server System. Microsoft Windows Server System makes Toyota Motor Sales USA's infrastructure easier to manage. Here's how: using Microsoft Operations Manager and Windows Server, Toyota has reduced the number of IT staff required to manage its dealer servers from seven to one, allowing the other six staff members to be redeployed to more strategic work. It's software that helps you do more with less. Get the full Toyota story and a hands-on management tool at microsoft.com/wssystem

Microsoft®
Windows Server System™

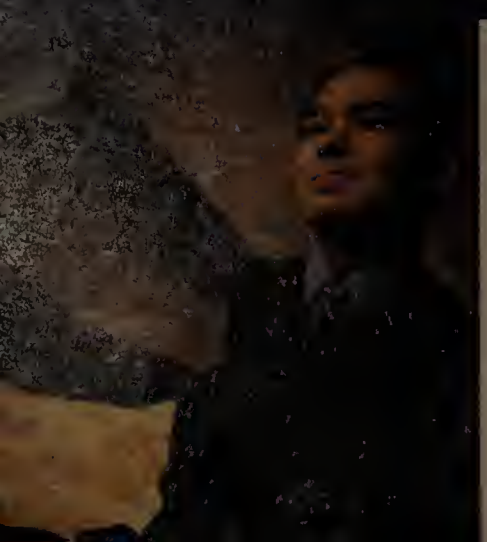
Windows Server System™ includes:

Server Platform	Windows Server™
Virtualization	Virtual Server
Data Management & Analysis	SQL Server™
Communications	Exchange Server
Portals & Collaboration	Office SharePoint® Portal Server
Integration	BizTalk® Server
Management	Systems Management Server
	Microsoft® Operations Manager
Security	Internet Security & Acceleration Server

Plus other software products

© 2004 Microsoft Corporation. All rights reserved. Microsoft, BizTalk, SharePoint, SQL Server, the Windows logo, Windows Server, Windows Server System trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products

CONSTANT.
CONTROL.



WITH THE DS SERIES, YOU ARE ALWAYS IN CONTROL.

Local data centers. Remote offices. Branch locations. They are all within your reach. The company who invented KVM over IP just made it better.

No more trips back to the office. With the all new DSView® 3 software, you can control servers and serial devices from a single browser interface – you can even power cycle or watch the servers reboot. Since we load balance user authentication for multiple sites, you get faster performance and quick access.

You know, you might even be able to take lunch. For a virtual tour of secure, smarter switching from Avocent, go online to www.avocent.com/control or call 1-866-286-2368.

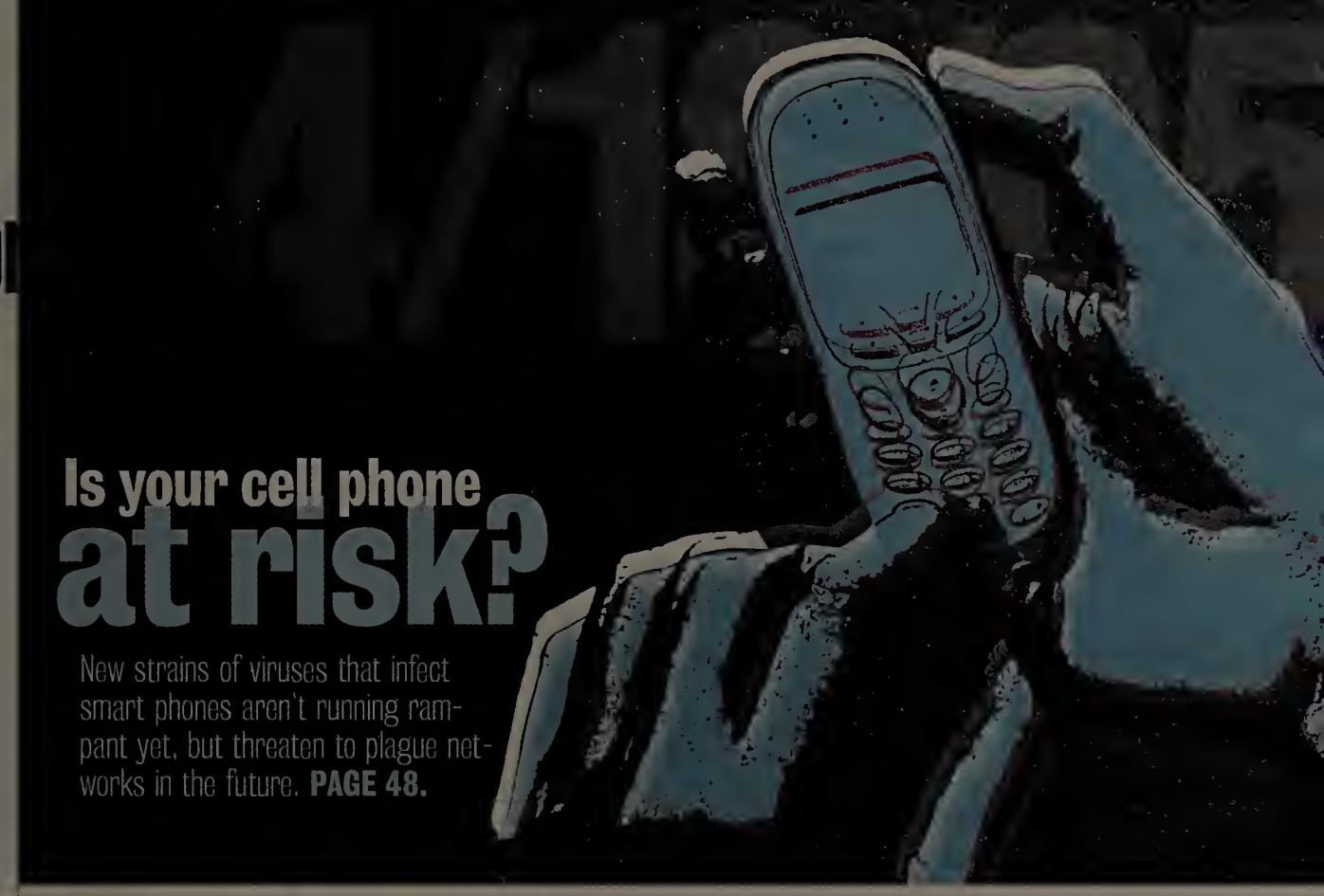
Avocent®
The Power of Being There®

Avocent, the Avocent logo, DSView and The Power of Being There are registered trademarks of Avocent Corporation. Copyright © 2005 Avocent Corporation.

Networ

News

- **8 Nortel** preps smaller IP PBX system.
- **9 Microsoft** to unveil parts to grander mgmt. plan.
- **10 Cisco upgrade** to meld storage-area networks.
- **10 Cisco routers** gain new IOS technology.
- **11** Big vendors vie for **RFID dollars.**
- **13** Do we need a **Sarbanes-Oxley** for the Internet?
- **61 HP** adds dual-core processor to Opteron blades.



Is your cell phone at risk?

New strains of viruses that infect smart phones aren't running rampant yet, but threaten to plague networks in the future. **PAGE 48.**

Net Infrastructure

- **17** Force10 crams switch full of Gig E.
- **17** Symantec readies anti-spyware products.
- **20** Start-up focuses on sharper video.
- **20** Uncertainty reigns in wireless world.
- **22 Special Focus:** Standard set to boost wireless QoS.

Enterprise Computing

- **25** Software tames thin-client setups.
- **25** Softricity touts Web-based app access.
- **27** Microsoft storage tool hits the beta stage.
- **27 Dave Kearns:** Compliance: A horse is a horse.

Application Services

- **29** Start-up to create open source harmony.
- **29** Software indicates when to discard information.
- **30** IBM software targets compliance.
- **30 Scott Bradner:** A target in your pocket.

Service Providers

- **35 Johna Till Johnson:** 911 isn't a negotiable added feature.
- **35** BT Infonet bolsters IP VPN services.
- **36** Legislation would prevent federal Internet access tax.

Net.Worker

- **39** Cisco aids government in business continuity.
- **39** Group tries to spur telework.

Technology Update

- **41** Category 7 cabling boosts throughput.
- **41 Steve Blass:** Ask Dr. Internet.
- **44 Mark Gibbs:** Open source opens opportunities.
- **44 Keith Shaw:** Cool tools, gizmos and other neat stuff.

Opinions

- **46 On Technology:** Why complexity is the next killer app.
- **47 Ira Brodsky:** Looking beyond 3G wireless.
- **47 Thomas Nolle:** Martin's FCC: More of the same?
- **62 BackSpin:** Forced to upgrade without complaint.
- **62 'Net Buzz:** Stealing at Internet2 speed.

Management Strategies

- **55** The IT apprentice: The state of North Dakota taps training program for help with network overhaul.

■ **CONTACT US** Network World, 118 Turnpike Road, Southborough, MA 01772; **Phone:** (508) 460-3333; **Fax:** (508) 490-6438; **E-mail:** nwnews@nww.com; **STAFF:** See the masthead on page 14 for more contact information. **REPRINTS:** (717) 399-1900

SUBSCRIPTIONS/CHANGE OF ADDRESS: Phone: (508) 490-6444; Fax: (508) 490-6400; E-mail: nwcirc@nww.com; URL: www.subscribenw.com

CLEAR CHOICE TEST

IP telephony systems: Aastra's peer-to-peer telephony system offers plug-and-play VoIP. **PAGE 52.**

Online: www.nwfusion.com

Breaking News

Go online for breaking news every day. **DocFinder: 1001**

Available only on Fusion

Network World Radio: Broadband without wires

How does a fixed wireless ISP differ from a traditional wire-based service provider? To find out, we talk with Graham Barnes, CEO of NextWeb, a wireless ISP in California.
DocFinder: 6740

Case studies

Learn best practices from your peers to make the most of technology, save money and streamline your business.
DocFinder: 6741

***Network Life*: Spotlight on home networks**

Keeping home networks free from viruses, bugs, spyware and worms isn't easy. *Network Life* offers strategies on securing your home network; 10 ways to stop spyware; tests of a wireless LAN security system and a WLAN extender. **DocFinder: 6451**

Network white papers

Want a vendor view on the up-and-coming network technologies? Head to our white paper library, featuring reports categorized via topic, company, date and more. **DocFinder: 6742**

Seminars and Events

WANs: Optimizing your network now

A new Technology Tour Event and Expo packed with immediate-impact ideas, information and strategies to help you optimize the business applications necessary to your company's success. Find out how you can qualify to attend free. **DocFinder: 6748**

Free e-mail newsletters

Sign up for any of more than 50 newsletters on key network topics.
DocFinder: 1002

What is DocFinder?

We've made it easy to access articles and resources online. Simply enter the four-digit DocFinder number in the search box on the home page, and you'll jump directly to the requested information.

Online help and advice

Nutter's Help Desk

Keeping an Internet connection secure

Help Desk guru Ron Nutter offers suggestions to a reader who's concerned about maintaining the security of his routers now that his company is moving over to a managed service offering: "What are some options to maintain the work I have done as we make the change to the new ISP/Internet connection?"
DocFinder: 6743

Gearblog

Web analysis and the 2005 Emetrics Summit

Network World Gearhead and BackSpin columnist Mark Gibbs writes: "The whole world of Web metrics has become a huge business in the last few years." He points you to a useful article by Brandt Dainow, CEO of Think Metrics, on the accuracy of measuring how people interact with Web sites — a topic otherwise called Web metrics.
DocFinder: 6744

Telework Beat

Struggling to stay open

Net.Worker Managing Editor Toni Kistner examines alternate work space theOffice as it fights for its life.
DocFinder: 6745

Home LAN Adventures

Our network gets a Webcam

Columnist Keith Shaw says the Actiontec 802.11g network camera delivers good quality video and strong security.
DocFinder: 6746

Small-Business Tech

Embarrassing security secrets

Columnist James Gaskin shows you the stupid things big companies do and how to avoid the same mistakes.
DocFinder: 6747

News Bits

IBM earnings rattle Wall Street

■ IBM late last week knocked Wall Street for a loop by announcing first-quarter earnings significantly short of analysts' expectations, in a report that came two business days ahead of schedule. IBM said its first-quarter earnings were 85 cents per share, below the 90 cents per share analysts forecast. Net income was $1.4 billion, on revenue of $22.9 billion, both up 3% from last year's first quarter. Analysts were expecting revenue of $23.6 billion. "After a strong start, we had difficulty closing transactions in the final weeks of the quarter, especially in countries with soft economic conditions, as well as with short-term Global Services signings," IBM CEO Sam Palmisano said in a written statement. IBM's Global Services revenue for the quarter, which ended March 31, came in at $11.7 billion, up 6% from last year. Hardware was essentially flat, at $6.7 billion, while software grew 2%, to $3.5 billion.

Science foundation funds security center

■ The National Science Foundation, the federal agency that funds science and technology research, last week announced a multimillion-dollar grant to the University of California, Berkeley, to establish a "cybersecurity Science and Technology Center." The center is intended to lead development of technologies to counter cyberattacks and better protect organizations against intrusions and fraud. The facility, expected to receive about $15 million over five years, also will research ways to ensure data trustworthiness through encryption.

Cisco warns of router vulnerability

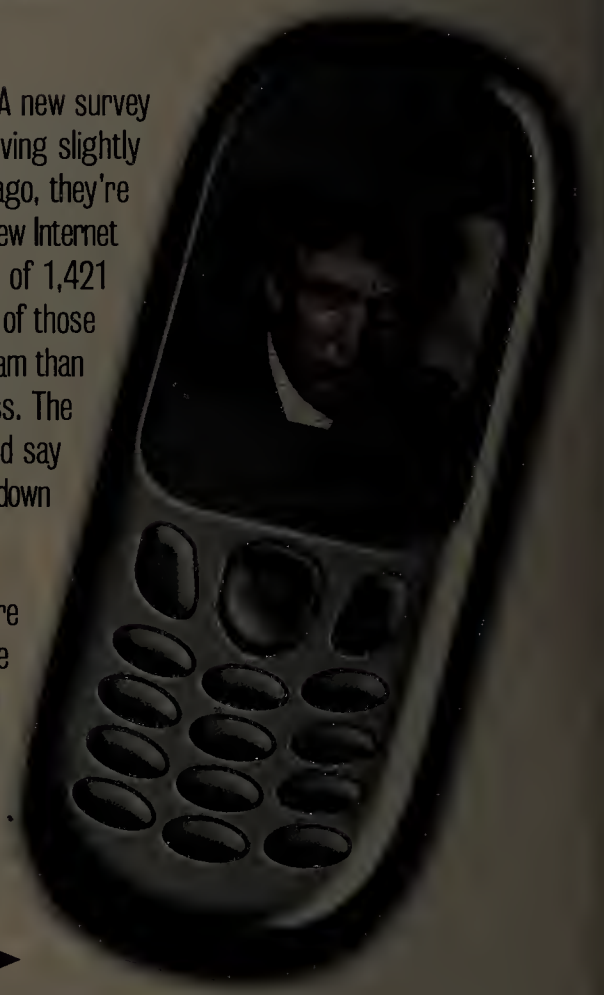
■ Cisco last week warned that a common management protocol used on the Internet could be used to launch denial-of-service attacks against Cisco routers and other IP-based gear. The security advisory warns of potential attacks based on Internet Control Message Protocol, which could make an IOS-based device inaccessible. The Cisco advisory is based on a bulletin posted by the U.K.-based National Infrastructure Security Co-ordination Centre, which references a document published on the IETF's Web site describing how ICMP can be used to launch DoS attacks against TCP traffic in general. ICMP is a protocol used with TCP/IP to alert devices of network outages and report diagnostic information to peer devices on an IP network. Cisco has released software fixes for the vulnerability.

"The new Xerox Workcentre Pro with optional USB Interactive Document Juggler!"

Layer 8 **Martin Zapata of Anaheim, Calif., wins top honors for submitting the above and winning our latest Weekly Caption Contest. Check in every Monday for the start of a new contest. www.nwfusion.com/weblogs/layer8**

TheGoodTheBadTheUgly

Coping with spam. A new survey finds that while people are receiving slightly more spam than they did a year ago, they're also a bit less bothered by it. The Pew Internet & American Life Project survey of 1,421 people concludes that 28% more of those interviewed are receiving more spam than a year ago vs. 22% receiving less. The survey shows 67% of those asked say spam makes being online annoying, down from 77% last year.



Tuning out. Cell phones are getting more feature-rich all the time, but not every new feature will be a winner. Only 12% of the 739 users surveyed recently by In-Stat say they are interested in buying cell phones capable of receiving TV broadcasts. (See story on cell phone viruses, page 48.) ➤

BMC blues. BMC Software will lay off between 825 and 875 employees, or about 12% of its global workforce, as part of a plan to reduce costs and improve its bottom line, the maker of systems management software announced last week.

Cisco snaps up Topspin

■ Cisco last week said it has agreed to buy server network equipment provider Topspin Communications for $250 million in cash and options. Topspin, in Mountain View, Calif., sells programmable server switches used in systems from vendors including Dell, HP, IBM and Sun. Buying Topspin adds to Cisco's portfolio a line of InfiniBand switches, which Cisco previously lacked. Five-year-old Topspin has a staff of 135 in Mountain View and Bangalore, India. Cisco, in San Jose, plans to add Topspin to its Data Center, Switching and Wireless Technology Group, headed by Luca Cafiero. With more customers building server architectures incorporating blades, grid computing and clustered applications, Cisco needs to deliver technology such as Topspin's server fabric switches and virtualization software, Cafiero said in a written statement.

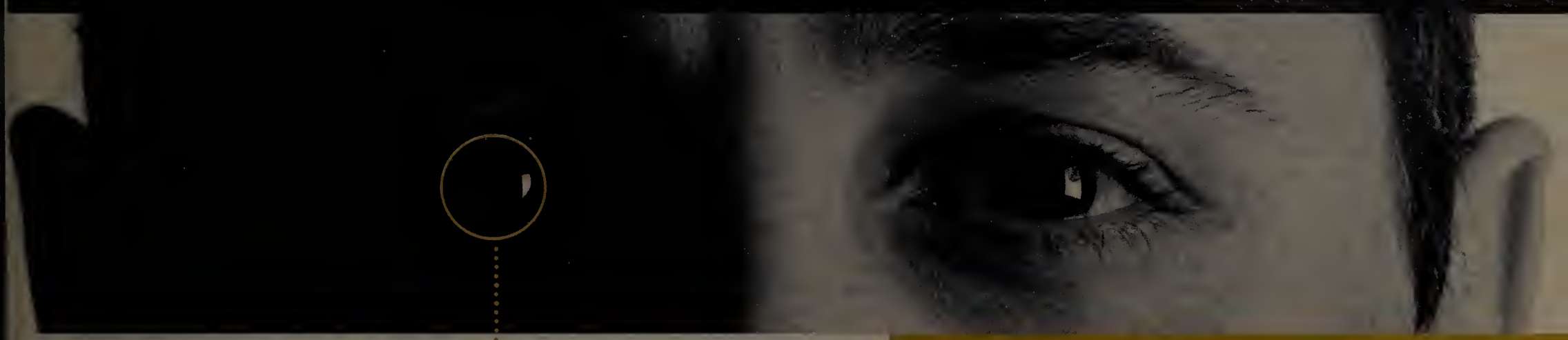
AOL advances IM interoperability

■ AOL is launching a program to make its AIM and ICQ instant-messaging services interoperable with enterprise IM systems from other vendors. Through the Enterprise Federation Partner program, AOL says it wants to make it possible for users of various enterprise IM systems to add AIM and ICQ users to their IM contact lists and vice versa, and let them exchange messages. Along with the launch of the EFP program, AOL is announcing four partners whose enterprise IM systems will interoperate with AIM and ICQ: Antepo, Jabber, Omnipod and Parlano. Notably absent from the program so far is IBM, whose Lotus Sametime is a major enterprise IM system, which several years ago interoperated with AIM but not anymore. Until now, the most common way to link AIM with enterprise IM systems has been through third-party gateway software work-arounds, which can be complicated to implement and sometimes yield unreliable performance.

One mighty cold hot spot

■ Two employees at Intel Russia have erected what could be the world's most northerly Wi-Fi hot spot — about 81 miles from the North Pole. The hot spot was built in the Arctic Region at the Barneo Ice Camp, a tent complex used by scientists, researchers and rescue crews during the month of April, when ice conditions are safe. Despite the challenges, the employees installed an 802.11b/g access point at the camp's headquarters, and then established a wireless LAN using four laptops with Intel's Centrino mobile technology, the company says. Another computer was placed outdoors and connected to a satellite phone to provide the network with Internet. The hot spot could be accessed by anyone at the camp who had a mobile or pocket PC.

Controlling outcomes is just a matter of wired and wireless Network SuperVision™ with one integrated tool



OptiView Series II™
Integrated Network Analyzer

Our new OptiView Series II Integrated Network Analyzer shows you more of what's happening on your network than you may have ever seen before. And faster. The graphic user interface and information-rich front page shows what's happening everywhere on your network in seconds flat – even on wireless, WAN and VLAN segments. Analyze 802.11 a/b/g WLANs just like you analyze your wires. That's troubleshooting with super vision. But it's not all. OptiView also gives you powerful monitoring and analysis capabilities to optimize your network performance. In fact, it's the world's only integrated tool that combines all three – troubleshooting, monitoring and analytical capabilities – into a single portable unit.

Seeing is believing. Go to www.flukenetworks.com/optiviewdemo and imagine the awesome control it puts in your hands.

FLUKE networks

NETWORKSUPERVISION™

2004 Fluke Corporation. All rights reserved. 01840

Nortel preps smaller IP PBX system

Linux-based VoIP box gives a glimpse into vendor's IP PBX road map.

■ BY PHIL HOCHMUTH

Nortel next month is expected to launch the first in a family of Linux-based IP PBXs that ultimately could save customers money, simplify management and ease application development.

The Business Communications Manager (BCM) 50, which the company plans to show next month at NetWorld+Interop in Las Vegas, is a scaled-down addition to Nortel's BCM product line, with a target deployment of 20 to 50 users. Nortel says the device fills a gap in its VoIP menu, where smaller customers were sometimes forced to buy larger systems than they needed.

The BCM 50 will run on Nortel Corporate Linux, a version of the open source operating system Nortel developed to run VoIP. This operating system will be the platform for future versions of all BCM products and Nortel's Communication Server 1000 IP PBX for large-enterprise deployments, the company says.

"Linux is an initiative you'll see us moving to across our enterprise portfolio," says Richard Solosky, a Nortel marketing director. He says the next software upgrade for all BCM products, Version 4.0, will be based on Nortel Corporate Linux. The Communication Server 1000 also will be migrated to Linux in its next major software release, due later this year.

With the BCM 50, Nortel is following the Linux lead of IP PBX vendors such as Alcatel, Avaya and Mitel Networks, and smaller vendors such as Zultys Technologies. Cisco, which runs its market-leading CallManager IP PBXs on Windows servers, also is expected to announce a Linux-based version of the product sometime this year.

Solosky says the move to Linux will give Nortel one operating system for all its convergence gear. Currently, the company runs the real-time VxWorks operating system on the Communication Server and embedded Windows NT on the BCM. Linux will let users work with one operating system across multiple Nortel voice platforms, while making it easier for Nortel to support the products. Third-party software developers and integrators also will have an easier time writing Nortel-based convergence applications for a single operating system, he adds.

The BCM 50 might find a place in the network of Global Materials Technology, a manufacturing company in Palatine, Ill., with offices worldwide. The company uses a BCM 400 in its headquarters to tie together plants throughout the U.S., China and Europe over VoIP.

Putting a BCM 50 in some of the company's plants as a local phone switch might make sense, whereas a larger BCM might be overkill, says Ed Jones, vice president of IS at Global Materials. Plants are currently connected using IP-enabled legacy PBXs or IP handsets and softphones, which link back to the central BCM 400.

The current Windows NT-based BCM platform has been trouble-free for Global Materials. "Both the embedded Windows NT and Linux platforms are stable platforms," Jones says. "But I think the Linux has a much better security background on it."

He cites the numerous security warnings and patches that are released for Windows servers as being a cause for concern.

The city of Richardson, Texas, which has a large IP-enabled Nortel PBX deployment, currently runs many of its IT applications on Linux servers. Moving telephony to the platform would be a positive thing, says Steve Graves, the city's CIO.

"From what we've seen, once you've installed a Linux machine, except for doing patches or updates, they just run and they're solid. I think it's a good idea for [Nortel] to move to that platform," he says.

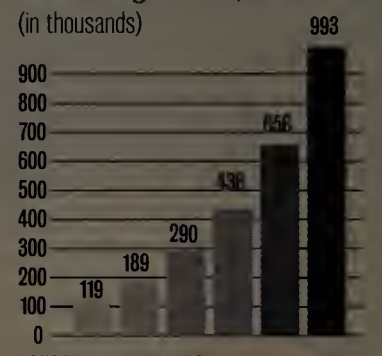
Another Nortel user also sees Linux as the way of the future for IP-based phone systems. But he questions the blanket assumption

See Nortel, page 10

SMB's take on VoIP

Small and midsize businesses (firms with fewer than 1,000 employees) will drive the market for converged phone systems in the coming years.

SMBs using IP PBXs, worldwide:
(in thousands)



SOURCE: AMI PARTNERS

AT&T
continued from page 1

conferencing and toll-free services over AT&T's IP infrastructure.

Although these IP services will be new to AT&T, the carrier is not the first to roll out such offerings, says Counse Broders, principal analyst for Internet and managed services at Current Analysis. "AT&T has a strong brand and significant network reach. They can come in and make a pretty big splash with these services," Broders says.

AT&T is moving traditional TDM services to its MPLS network to offer "economic advantages," Antieri says. "IP conferencing is an example of a plug-and-play application that [AT&T] is making available to customers."

Instead of developing applications in-house, Antieri says AT&T is using off-the-shelf software and making it available to customers. The carrier says it is testing these services with customers, but would not reveal details.

AT&T's IP conferencing service will eliminate transport costs for users by keeping audio traffic on its MPLS network, Antieri says. "Instead of transporting calls to TDM, calls are routed over IP eliminating transport costs," he says.

United Communications Group (UCG), a Rockville, Md., company that uses AT&T's managed MPLS IP VPN service to securely connect seven locations in the U.S., says it sees value in AT&T's planned offerings.

"Internally we don't use a lot of audio conferencing, but we do host a lot of audio conferences for our customers," says Mitch Barlow, CTO at UCG, which provides business-to-business content to users in industries such as healthcare, oil and energy, and education.

IP conferencing would only be advantageous to UCG if AT&T was going to offer local dial-in numbers for all locations, Barlow says. Without that, UCG still would have to pay transport costs. "I could see a time when that would happen, but I'm not sure [local dial-in support] will be part of AT&T's offering," he says.

AT&T says only that more details will be available when it makes an official announcement later this year.

Antieri says the nature of MPLS makes it an ideal platform to support multicasting and data streaming, which is why the carrier plans to introduce IP video.

UCG uses videoconferencing gear in-house and sends that traffic over its MPLS VPN. The company uses three classes of service to prioritize traffic over its VPN. Video traffic is dedicated to the second class, after voice but before data.

Video units cost about $5,000 to $6,000 and are easy to use, set up and support, Barlow says. "There are economies that don't make sense for me to move to IP video. I've already made a minimal investment in video gear," he says.

"If there was a feature benefit I would consider it," he says. "If I could hook each desktop into the system where I could broadcast to everyone in the company, that would be part of a feature-rich environment I'd like."

Barlow also says that if he didn't already have a videoconferencing environment or if his gear was old, he would seriously consider the service.

One vendor that already offers IP videoconferencing services is GlowPoint. According to analyst Broders, the GlowPoint service is user-friendly and provides help for when conference problems arise. "Users just have to dial 000 # and a live operator will come on the line," he says. "Those who aren't tech-savvy want easy set-up and technical assistance." As AT&T and its competitors start rolling out IP video services, those are features they should emphasize, he adds.

AT&T will be behind the pack with its IP Centrex services. BellSouth, Qwest, SBC and MCI all have IP Centrex offerings today. Verizon is expected to roll out such an offering next quarter. And Sprint says its offering will be available this sometime this year.

AT&T will offer users a hosted IP Centrex service, which will include PBX-like telecom features off-site and over a user's MPLS VPN. Typical IP Centrex features include click-to-dial, find me/follow me, IP conferencing, call blocking, call forwarding, voice mail and caller ID.

ServiceMaster, which just announced a $21 million contract with AT&T last week, doesn't plan to deploy AT&T's planned IP services over its MPLS VPN. But it likes that AT&T will have these capabilities going forward, says Jim Goetz, CIO at ServiceMaster in Downers Grove, Ill. "We think strategically MPLS is the right platform to support more advanced applications," he says.

"We do have an interest in video, but it's not even in pilot yet," Goetz says. But one reason ServiceMaster switched from a frame relay network to an MPLS VPN was to have the ability to eventually support a variety of applications, he says.

The company is deploying a Cisco-based VoIP system. "Let's assume we survive voice, then we'll start thinking about other applications," he says. ■

TDM to IP

Carriers are offering or readying a host of IP services that bring legacy applications to IP networking.

Provider	IP video	IP conferencing	IP Centrex
AT&T	Second half 2005	Second half 2005	Second half 2005
MCI	Available	Available	Available
Sprint	Available	No	Year-end
BellSouth	Available	Available	Available
Qwest	No	No	Available
SBC	Available	Available	Available
Verizon	No	No	Second quarter

Microsoft to unveil parts to grander mgmt. plan

System Center offerings to include capacity planning, back-up and recovery tools.

■ BY JOHN FONTANA

Microsoft this week plans to introduce a limited beta of a tool for capacity planning. It will be one piece of a broad suite of tools designed to help companies model, deploy and manage network resources.

The news is scheduled to be announced at the company's annual Microsoft Management Summit in Las Vegas, where 2,600 attendees are expected.

The suite is a departure from Microsoft's 2-year-old plan to offer a product called System Center 2005, which was slated to ship this fall, that would integrate System Management Server (SMS) 2003, Microsoft Operations Manager (MOM) 2005, a reporting engine and a modeling tool for capacity planning, which is code-named Indy.

Users can expect a cache of individual tools under the brand name System Center that will perform tasks such as change and configuration management, asset management, application management, IT process orchestration, performance trending, reporting, backup/recovery and capacity planning. The original plan was to build it all into a single infrastructure.

"Microsoft insisted that it is important to develop a management brand that can compete with Tivoli and Unicenter," says Peter Pawlak, an analyst with independent research firm Directions on Microsoft. "You will eventually see that name [System Center] applied to SMS and MOM."

Microsoft officials declined to comment on the company's System Center plans.

The first pieces of System Center trickled out in March with the beta release of Reporting Manager 2005, a tool that collects data from SMS and MOM and lets users generate reports that combine information from the two, such as configuration and overall performance.

Last week, the second System Center-branded tool emerged when Microsoft introduced Data Protection Manager, a diskless back-up and recovery server that was previously called Data Protection Server.

And this week, Indy is expected to take on the System Center moniker when independent software vendors are given the first feature-complete beta code at the Management Summit. The Indy modeling technology was developed by Microsoft Research. It lets users model a server deployment based on characteristics such as the number of offices and users. A simulation of user workload can be run to determine system capacity, letting users experiment with different hardware and software configurations and user behavior before deploying anything on a live network.

Microsoft plans to demonstrate at the Management Summit how Indy can aid in deploying Exchange Server 2003.

System Center is one piece of Microsoft's 2-year-old strategy called the Dynamic Systems Initiative (DSI), a 10-year plan to build a comprehensive management platform for Windows.

DSI is designed to give corporate users a range of assessment, configuration, monitoring, management and development tools that will support Windows-based software and let it communicate its status to the network as a way to automate and improve the security, uptime and general maintenance of Microsoft infrastructure.

DSI's utility computing design is targeted to compete with offerings from Computer Associates, HP and IBM.

"Microsoft is starting to expand out to areas where other management companies have been operating for quite a while," says Audrey Rasmussen, an analyst with Enterprise Management Associates. "One thing that would be good is to hear more about the strategy. As companies start to pull together product lines sometimes the vision shifts a bit, and Microsoft needs to articulate their vision in terms of management and where they are headed." ■

Network Management
Subscribe to our free newsletter.
DocFinder: 5434 www.nwfusion.com

and then it hits you://

HOW MANY FORMER EMPLOYEES

CAN STILL ACCESS YOUR COMPANY'S

INFORMATION?

Novell®

find out more at novell.com

©2005 Novell, Inc. All rights reserved. Novell is a registered trademark of Novell, Inc in the United States and other countries.

Cisco upgrade to meld storage-area networks

■ BY DENI CONNOR

PHOENIX — Cisco last week upgraded its storage-area network switches to let customers more easily consolidate their SANs.

At Storage Networking World in Phoenix, the company said the revision brings support for Fibre Channel network address translation (FC-NAT) to its MDS 9000 director-level and fabric switches. This lets Cisco SAN switches communicate with each other and with switches from other vendors even when the servers attached to them have the same domain ID. This identifier is the equivalent in IP networks to the device's IP address.

"If I don't use FC-NAT, I have to ensure unique Fibre Channel addresses across all virtual SANs," says Rajeev Bhardwaj, manager of product marketing at Cisco.

Cisco says this feature is especially helpful to companies that are trying to merge branch-office SANs or SANs they might have acquired through a company merger.

Paul Macht, senior IT architect for Duke Health Technology Solutions in Durham, N.C., uses Cisco's MDS 9500 Multilayer Director switch to sync up SAN islands.

"Most SANs that have been deployed over the last five years have used the default domain IDs of 20 and 10," he says. "Having duplicate domain IDs causes disastrous results for our systems that are providing ancillary critical care to Duke facilities."

FC-NAT is supported within Cisco's SAN-OS 2.1 operating system and in a dedicated ASIC.

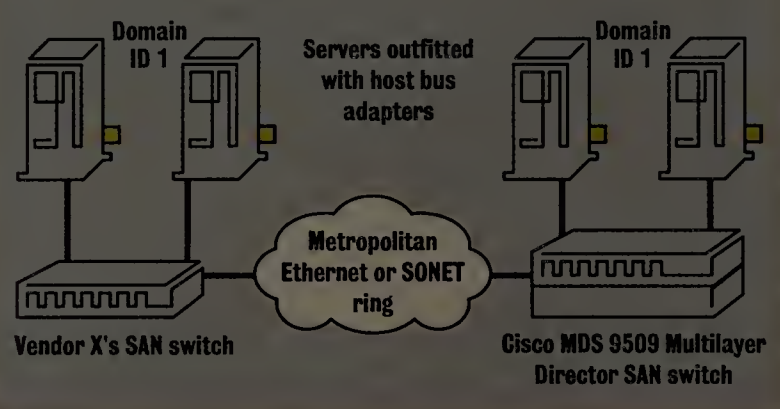
The technology brings Fibre Channel routing much closer to IP routing, which lets IT administrators without specialized storage training understand and implement it.

Cisco rivals such as Brocade Communications and McData also support FC-NAT, but Cisco is the first to support the technology across its entire SAN switch line.

In other news, Cisco announced that it has acquired InfiniBand product vendor Topspin Communications for $250 million. Cisco says it will add Topspin's products to its Data Center, Switching and Wireless Technology Group. ■

SAN-style network address translation

An upgrade to the operating system for Cisco's SAN switches is designed to ease consolidation of SANs, including those supporting servers that boast the same domain IDs (the SAN equivalent of IP addresses).



Nortel

continued from page 8

that this will lead to more secure systems.

"I think that more and more telecom managers are looking at Linux-based platforms," says John Tichenor, telecom manager at Chadbourne and Parke, a New York law firm with offices nationwide, which uses Nortel PBXs. "But are they doing this strictly because Linux has less security patches than Windows? The question is, if more telecom vendors go with Linux, do people who want to disrupt telecommunications then go and write more Linux viruses?"

One industry observer sees Windows and Linux as being on par in terms of reliability when deployed on IP PBXs. But there is still a stigma around Windows in the telecom realm.

"I haven't heard many horror stories lately regarding IP PBX uptime that can be traced back to problems due to Windows," says Brian Riggs, an analyst with Current Analysis. "But it is still the case in some larger enterprises that they tend to be fairly wary of running their voice network on a Microsoft platform."

The Linux-based BCM 50 will include support for up to 50 phones, which could include a mix of Nortel IP phones, digital handsets, PC-based softphones and analog lines. The device includes built-in voice mail (up to 1,000 mail boxes and 100 hours of recording) that can integrate into a Microsoft Outlook client for unified voice/e-mail messaging. The device has the option of including an integrated WAN router (with T-1 or DSL connection interfaces) as well as a VPN gateway and firewall, which lets users deploy a single box in a small office or remote site. Nortel says the BCM 50 will cost between $350 and $500 per user.

Later this year, Nortel says it will release a version of the BCM 50 called the Survivable Remote Gateway. This box will act as a local VoIP gateway for a remote office tied to a centralized Nortel IP PBX (such as a larger BCM or Communication Server 1000). The Survivable Remote Gateway will connect local IP phones to the main IP PBX, and provide local public switched telephone network connectivity and call control in case of an IP WAN link failure. ■

More online!

Discover the latest innovations rocking the world of WAN. Attend a special *Network World* event for network managers.

DocFinder: 6238

Cisco routers gain new IOS technology

■ BY JIM DUFFY

Cisco this week is expected to unveil the first evidence of stated plans to diffuse its next-generation routing technology throughout its product line.

The company plans to roll out a model of its 12000 series Internet routers that runs the company's modular IOS XR operating system that debuted almost a year ago along, with a new core router. Cisco also is set to unwrap a smaller version of its 7600 metropolitan Ethernet router, as well as interface card and module enhancements for its midrange and high-end carrier routers.

The expected product extensions (see story at www.nwfusion.com, DocFinder: 6749) could translate into more carrier service options for enterprise networks, as they will let carriers offer a broader range of services on a wider array of Cisco platforms. The enhancements also will help stabilize the IOS XR operating system by putting it in the hands of more carriers and in more production networks, analysts say.

Key move

"This is a very important thing for Cisco to do," says Mark Seery, an analyst at RHK. "Because the CRS-1 is going to take time to really evolve into a high-volume platform, getting IOS XR onto the 12000 form factor will accelerate the maturity of that software base. The CRS-1 is Cisco's top-of-the-line core carrier router.

The XR 12000 is essentially a 12000 series router with an IOS XR software upgrade. IOS XR brings a number of improvements to the 12000, which had been running Cisco's traditional IOS software, such as secure virtualization, continuous system operation and multiservice scale, Cisco says.

Secure virtualization is the key feature, as it lets service providers isolate public and private services in a single router into separate physical and logical routing domains.

"It allows them to have true separation of customers per virtual router," says Jennifer Liscom, an analyst at Gartner.

The operating system's modularity helps provide continuous system operation by isolating specific software components for upgrades or fixes without taking the entire router offline. The XR 12000 also enhances scalability of services such as frame relay, ATM, Layer 2 and 3 VPNs, queues and access control lists, Cisco says.

BellSouth is anxious to evaluate XR 12000 for edge-specific functions next year.

Time for change

"IOS is many, many years old, and it is an amalgamation of enterprise and carrier feature sets," says Mike Duckett, research director in BellSouth's science and technology group. "It's not very modular, it's high-risk for introduction of new functionality, it is not carrier-class."

Meanwhile, 7600 users can deploy the router in smaller points of presence now that Cisco has winnowed down the chassis to four slots. Larger customers requiring WAN aggregation at the edge of the network also can use the 7604.

The 7604 and XR 12000 routers — as well as those ranging from the 7300 to the CRS-1 — can run Cisco's new Shared Port Adapters and SPA Interface Processors (SIP). SPAs and SIPs are intended to provide broad interface options — such as copper, channelized, packet over SONET, ATM and Ethernet — for the Cisco carrier routing portfolio to reduce total cost of ownership for cross-platform sharing and sparing.

The XR 12000 is expected to be available in June. List prices for upgrade kits start at $10,000. The 7604 router is expected to be available by the end of the month. It's priced starting at $34,000.

The SPAs and SIPs are priced starting at $2,500 and vary according to product models and supported platforms. ■

Correction

■ In the stories "CA gobbles up Concord" (April 11, page 11), "Goodbye, NetWare; hello, Unicenter" (page 29) and the Good, the Bad and the Ugly on page 6, Computer Associates' President and CEO should have been listed as John Swainson.

Big vendors vie for RFID dollars

■ BY ANN BEDNARZ

With a blitz of new radio frequency identification products ready to ship, major platform vendors continue to bolster their efforts to make sure the wireless tracking technology is ready for corporate users to deploy.

This week Sun is expected to announce an upgraded version of its RFID middleware. Sun Java System RFID Software 2.0 features improved management tools designed to help users keep tabs on distributed sensor devices, along with built-in provisioning capabilities that let customers prioritize critical RFID-based processes.

Sun's news comes after a string of RFID-related announcements Oracle made last week, including a development partnership with Intel. Oracle also is teaming with RFID appliance maker Xpaseo to offer an integrated software and hardware package for managing RFID deployments.

Sybase also last week unveiled middleware designed to help companies incorporate data collected by RFID devices into business applications. RFID Enterprise bundles a range of data management, integration and analysis components, and includes hooks to a product Sybase subsidiary iAnywhere Solutions announced in February for RFID device management.

These vendors' latest product releases share an emphasis on enterprise-quality data management and integration — features that early adopters of RFID in supply chain settings are beginning to require.

Increasingly, consumer-goods companies are getting ready to make the shift from small, localized RFID pilots to multisite rollouts as the scope and number of RFID adoption mandates from retailers such as Wal-Mart, Best Buy and Albertsons expands, says Erik Michielsen, director of RFID and ubiquitous networks at ABI Research.

"RFID installations have not been networked or tied to mission-critical enterprise systems in most cases," Michielsen says. "As companies' needs start to get more complicated, they're going to start looking for centralized management capabilities so that single-location solutions can be tied together. That's an obvious place for vendors like Microsoft, SAP, Oracle and IBM to step in and provide integration between reader devices and enterprise systems."

At the same time, RFID adoption is gaining momentum outside retail and consumer goods industries, in areas such as healthcare, pharmaceuticals, and aerospace and defense. The growth is bolstering RFID technology-spending projections and enticing big IT vendors to deepen their RFID investments.

HP, IBM, Microsoft and SAP have added steadily to their RFID wares over the past several months. Most recently, SAP in March announced a program aimed at making RFID technology accessible to small and midsize businesses. SAP is teaming with a handful of RFID vendors to add automated data collection, wireless warehouse management and RFID data integration features to its Business One suite for small and midsize companies.

For its part, IBM last fall announced a five-year, $250 million investment to support a Sensor and Actuator Solutions division and 1,000 IBM employees working on RFID software, services and hardware projects.

Microsoft through its Business Solutions division is building RFID capabilities — including reader management and data translation features — into business management applications such as Axapta 4.0, Navision 5.0 and the next major release of its Great Plains software. ■

RFID technology spending on the rise

Global RFID hardware and software revenue grew from $1.25 billion in 2003 to $1.54 billion in 2004 and is projected to hit

$1.94 billion

this year, according to ABI Research.

and then it hits you://

RIGHT NOW YOUR COMPETITORS

ARE DISCOVERING LINUX, TOO.

Novell®

find out more at novell.com

©2005 Novell, Inc. All rights reserved. Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Vulnerable

continued from page 1

dedicated circuit to all these entities."

Clif Triplett, global technology information officer at General Motors, says he is worried mostly about router and host software bugs, as well as broadcast storms such as distributed DoS (DoS) attacks bringing down the 'Net.

"I'm highly concerned about it," Triplett says. "If that network is a core piece of your business, I think you're at a risk."

These IT professionals are not alone. Two-thirds of the 1,300 "technology leaders, scholars and analysts" surveyed recently by the Pew Internet & American Life Project said they "expect a major attack on the Internet or the U.S. power grid within the next 10 years."

Experts warn that the 'Net is particularly vulnerable in these areas:

- DNS root servers.
- Border Gateway Protocol (BGP) peering points.
- Individual router and switch elements.
- Host/endpoint operating systems.

The root of the problem

The 13 DNS root servers resolve Internet naming and addressing. If they were knocked out, Internet sites would become inaccessible.

The servers repel distributed DoS attacks every day, operators say. CAIDA research shows that up to 85% of the queries against the DNS servers are "bogus" or repeated from the same host.

The system has been bolstered since the 2002 attack, with root servers now consisting of 50 to 100 physically distributed, highly redundant boxes in 80 locations across 34 countries. In 2002, far fewer servers were located in 13 sites across four countries.

This level of distribution and redundancy makes a complete shutdown of the DNS system unlikely, says Paul Mockapetris, chairman and chief scientist of IP address management vendor Nominum and the inventor of DNS.

The physical servers use Anycast, a routing technique that heightens resiliency by multiplying the number of servers with the same IP address and balancing the load across an army of geographically dispersed systems.

"If I was going to try and arrange a DNS 9/11, it's a very bad target to try and attack because it's so distributed — you'd have to take [the servers] out everywhere," Mockapetris says. "If you took out one root server today, nobody would notice."

But the more distributed a system is, the more difficult it is to defend, notes Stephen Cobb, an independent security consultant who was recently quoted in a *Network World* column stating a belief that the 'Net can be brought down and kept down for 10 days or more. Cobb say the 'Net is up only because of the moral high ground of those who know how to bring it down.

"I just don't think technologically we can ever harden the Internet to where it's invulnerable to intelligent, determined people," he says. "The reason it hasn't gone down for days so far is that the people who know how to do it aren't so inclined."

However, the good guys are inclined to implement security best practices, like those outlined in an IETF informational document on root server operation called RFC 2870, says Jose Nazario, security researcher and senior software engineer at Arbor Networks, which makes products carriers use to protect their networks from cyberattacks. Originally drafted in 2000, RFC 2870 has been extended over the past couple of years.

Even so, experts don't discount the possibility of another attack equal to or exceeding the scope of the October 2002 event. But they also are confident that the DNS root servers and Internet users will experience minimal disruption.

"There's no way to get them all with truck bombs; there's no way to get them all with a single attack; and there's no way to keep an attack going long enough that I could not usefully counteract it," says Paul Vixie, president of the Internet Systems Consortium, which also operates the DNS F root server. "It's better for me to simply not accept any traffic from [the attacker] even though I will be losing a certain number of Web hits. As soon as you rendered the attack worthless, then it's actually in the attacker's best interests to stop launching it because otherwise you will trace it back."

The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for top-level coordination and global policy-making for the DNS, and plays a central role in assuring the integrity and stability of the system.

"Taking out the whole Internet for 10 days — I'm a little skeptical," says Steve Bellovin, a computer science professor at Columbia University, former researcher at AT&T Labs and a member of ICANN's Security and Stability Advisory committee. "If you look at the kinds of attacks we've had thus far — worms and [distributed] DoS attacks — many of these things have had noticeable impact in the short run but they weren't too hard to counter."

Routing around catastrophe

Bellovin and others are not as confident about the routing infrastructure. Cisco, the leading provider of Internet routers, regularly issues bug alerts. And BGP, which distributes routing information between networks on the Internet, is susceptible to IP address spoofing.

"BGP peering has some security problems," says Sam Hartman, area director for the IETF's Security Area working group. "What's there now is hard to configure, and it's something that the community has identified as a real problem. You're not just depending on the security of the person you're directly connected to; you're also depending to some extent on the security of the people that are connected to them."

Work has been underway for a while on methods to authenticate BGP route advertisements. Secure BGP (S-BGP) has been incubating for more than eight years and its alternative, Secure Origin BGP (soBGP), is also a multiyear effort. Yet these proposals are not implemented because router vendors have not incorporated them into their products — they say BGP already has enough integral security features that can be exploited through proper implementation.

There also are concerns among service providers about router load and overhead and the effect on customer service-level agreements from weighty specifications such as S-BGP and soBGP.

"The workload gets significantly higher, and it's kind of a turnoff for the people who are not major core operators," Arbor's Nazario says.

Many ISPs implement TCP MD5 cryptographic hashing (RFC 2385) to authenticate BGP data. But it's not a mandate. Operators can choose not to turn on the techniques for various reasons, such as router performance degradation.

"But [MD5] is easy to deploy in a hurry if the link starts being attacked," says Scott Bradner, university technology security officer at Harvard University and a network design and security consultant. Bradner is also a *Network World* columnist.

IPSec also can be used as an alternative to MD5 to add some level of protection to the BGP transport connection, experts say. Operators can implement infrastructure access control lists, BGP/Generalized TTL Security Hack — which is designed to protect against CPU overload-based attacks — prefix filters and priority queuing for control plane traffic, they say.

There also is an informational IETF document — RFC 3882 — on configuring BGP to block DoS attacks.

Hardware needs hardening

Routers themselves also are patched quickly when software bugs are discovered, Bradner says, despite — and thanks to — the frequency at which they occur. Cisco has regularly reported distributed DoS vulnerabilities in its IOS software over the years. But the fact that the vendor has reported them and recommended patches in a timely manner has helped keep disruptive events to a minimum.

Still, that's little solace to GM's Triplett. He says more and more telecom operators run the latest versions of routing software not only to get new features but also to maintain release consistency to better alleviate bugs.

But the latest software is usually the buggiest — the Release 1.0 conundrum.

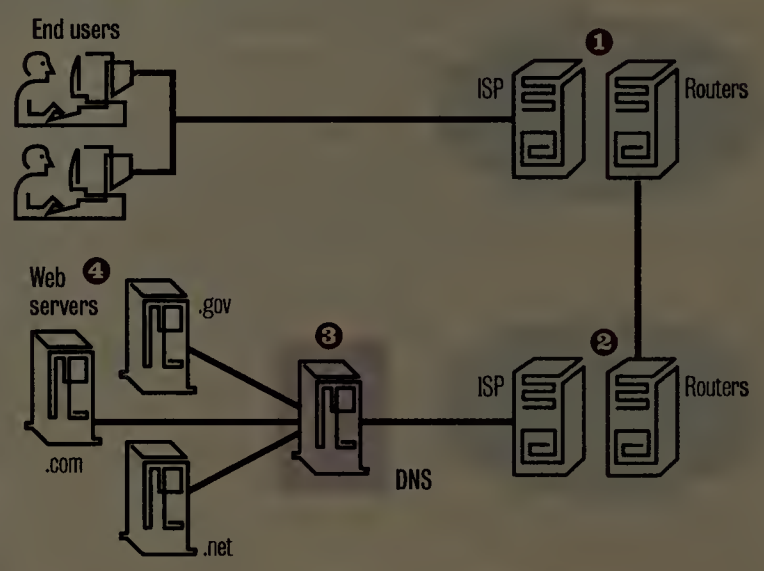
"This is kind of a Catch-22 situation," Triplett says. "All of a sudden, if they all get on the same release ... you can almost start having an effect similar to what we saw on the power grid" in the Northeast two years ago, with the ripple effect electrical blackout.

For that reason, Triplett and other experts consider the 'Net's

See Vulnerable, page 15

Fixing the 'Net

Four areas where efforts are being made to boost Internet security.



1 Routers:
- Cisco and Juniper bug alerts are posted on accessible security sites such as US-CERT.
- The IETF's Routing Protocol Security working group publishes documents on generic threats and security requirements for routing protocols.

2 BGP peering:
- Work continues on Secure BGP and Secure Origin BGP to authenticate route advertisements.
- Some ISPs use TCP MD5 cryptographic hashing to authenticate BGP data.
- IPSec, infrastructure access control lists, BGP/Generalized TTL Security Hack prefix filters and priority queuing for control plane traffic can help protect BGP connections.
- The IETF RFC 3882 document on configuring BGP to block DoS attacks was published last fall.

3 DNS root servers:
- Operators have installed scores of redundant, distributed services to thwart distributed DoS outages.
- 13 groups of servers use Anycast routing to share a single IP address.
- The IETF RFC 2870 document outlines best practices for DNS root server operators.
- Operators counteract suspicious activity by blocking traffic from attackers or tracing it back to them.

4 Host operating systems:
- SANS Institute publishes annual list of Top 20 operating system vulnerabilities for Windows and Unix/Linux.
- Microsoft has been investing heavily in patching tools and anti-virus companies.
- Open source software suppliers continue to develop patch management tools.

Do we need a Sarbanes-Oxley for the Internet?

■ BY JIM DUFFY

Should there be a higher authority for Internet security?

With billions of dollars transacted daily via the Internet and online banking growing, some say it's high time for industry to collaborate on a stringent security doctrine to hold organizations accountable for operating, providing and commercializing Internet service.

"I'm held to accountability through Sarbanes-Oxley (SOX) and all these other regulatory requirements," says Larry Jarvis, vice president of network engineering for Fidelity Investments. "That doesn't exist for some of these critical elements in the Internet."

Jarvis recommends forming and funding a joint commercial/governmental/academic body to define and enforce security standards for the Internet. But Internet security experts say previous attempts have failed because of the evolving nature of computer and network security technology.

"I think it would be impractical," says Steve Bellovin, a computer science professor at Columbia University and a member of the Internet Corporation for Assigned Names and Numbers' Security and Stability Advisory committee. "The track record of the industry in evaluating stuff against security guidelines is not good. It's very difficult to get a system certified, and once you get something certified it's obsolete. If nothing else, computer systems don't stand still."

Some smaller, specific procurement-focused edicts have worked, says Alan Paller, director of the SANS Institute for security training, certification and research. Paller cites the $500 million U.S Air Force contract awarded to Dell and others last year for systems that complied with the Air Force's security and patching requirements (www.nwfusion.com, DocFinder: 6727).

The Air Force specification, developed with guidance from the Center for Internet Security, will lower the cost of patching by $100 million by eliminating 85% of known vulnerabilities, according to CIS.

"In war, Patch Tuesday doesn't sound real good," he says, referring to Microsoft's monthly issuance of software fixes. "I can't imagine a large company being not at least interested in following this."

Paller also is a member of the procurement subgroup of the Corporate Information Security Working Group (CISWG) of the Institute for Internal Auditors, which recommends procurement guidelines and best practices for improving information security in the public and private sector. CISWG comprises 25 senior officials from business, academia and elsewhere, and is chaired by Rep. Adam Putnam (R-Fla.), chair of the U.S. House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.

"That is the industry/governmental collaborative effort" for Internet security, Paller says, but adds that the controversial body's recommendations have been "softened over and over again."

Another group that recommends best practices for secure IT procurements is BITS, a nonprofit, CEO-driven financial service industry consortium made up of 100 of the largest financial institutions in the U.S. Its Security and Risk Assessment (SRA) Working Group shares best practices and strategies for developing secure infrastructures, and promotes compliance with security requirements before software products are released. The organization also conducts product testing and certification against baseline security criteria established by the industry.

Best practices — scores of them, from organizations such as CISWG, CIS, BITS and the IETF — will have to do until an organization attempts the gargantuan task of defining an overarching Internet security framework. Some feel the ultimate coordination for Internet security will default to the federal government — specifically to SOX.

"Sarbanes is going to figure it out in the not too distant future: They need to look at the networks," says Clif Triplett, global technology information officer at General Motors. "If the network is one of the key elements of [our] business . . . we're thinking that this Sarbanes-Oxley thing is going to grow in scope over time." ■

and then it hits you://

SECURITY ISN'T ABOUT KEEPING

PEOPLE OUT. IT'S ABOUT LETTING

THE RIGHT PEOPLE IN.

Novell®

find out more at novell.com

©2005 Novell, Inc. All rights reserved. Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Hermosa Beach

continued from page 1

community of about 19,000 people. While far removed from high-profile political battles in states such as Pennsylvania and Texas over whether municipal networks should be encouraged or restricted, Hermosa Beach has become a case study of the dictum by the late U.S. House Speaker Thomas O'Neill that "All politics is local."

Here, technology issues are intimately wedded to ideas about the proper role of government, business and citizenship, and about municipal priorities.

During a contentious January meeting, as reported by the local *Easy Reader* newspaper, Councilman Michael Keegan accused Councilman Sam Edgerton of not supporting the network "because you don't understand it." Edgerton told the audience: "This guy's like a rabid dog."

Two councilors say "yes" to creating a city-wide wireless network, two say "no," and one, who works for telecom vendor Cox Communications, abstains. The deadlock isn't expected to be broken until November, when wireless advocates face re-election and voters could face ballot questions. The council voted last week to have City Manager Steve Burrell draft two ballot measures: one to approve a free wireless network, another to determine if residents are willing to pay for it.

Making arguments

The network, dubbed Wi-Fi Hermosa, is the brainchild of Keegan, who runs a bakery at nearby Manhattan Beach. He calls himself a "self-taught Wi-Fi expert" who became interested in WLANs after reading a newspaper story. He set up an access point at the bakery and plugged it into a DSL line. Customers began using it, and word of mouth drew more users.

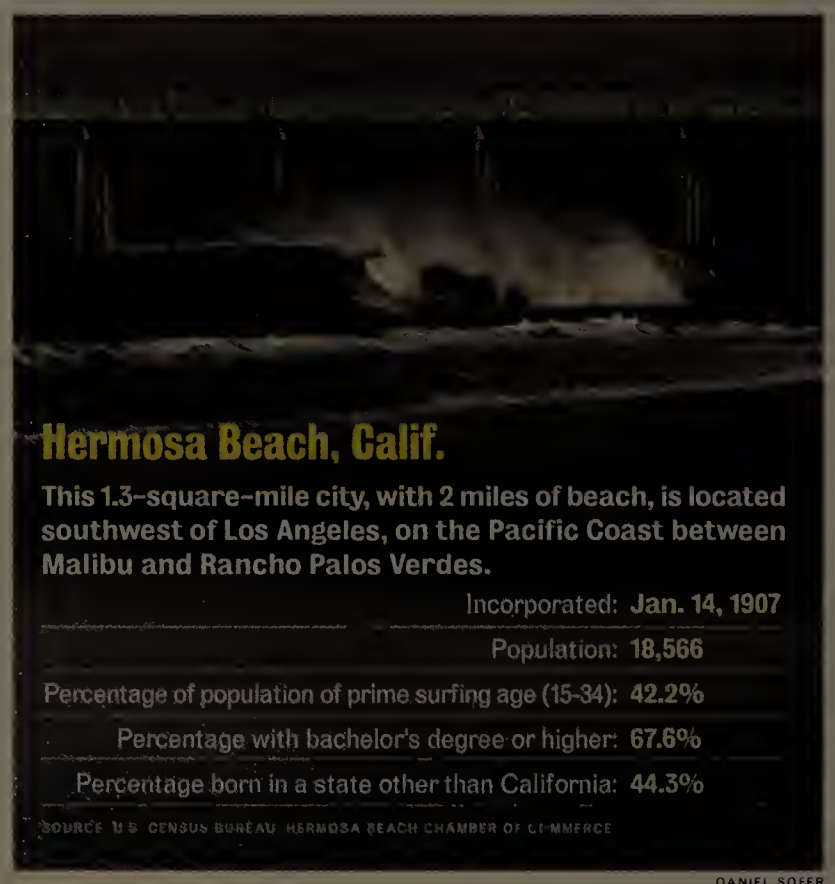
To Keegan, it seemed a simple matter to build a similar network that could do the same thing for all of Hermosa Beach.

"We already fix the roads, pick up trash, have concerts in the park and classes to teach you to dance," he says. "The Internet is like these. It's pretty close to being something that people will expect to have. It's close to being an essential service."

Nowhere near close enough, says Peter Tucker, a councilman opposed to spending money to extend the network. He says the city is strapped for cash and faces state-mandated upgrades to its aging infrastructure.

"I have to be able to look you in the eyes, and say 'We're not going to pay to improve your street, but we are going to give you free Wi-Fi,'" Tucker says. "You have to prioritize your needs and wants. This free Internet stuff would be way down on my list."

Tucker and Edgerton worry that other radio technologies such as WiMAX would make the network obsolete, that future upgrades will be costly and that the city might face legal liabilities. Keegan and fellow Councilor and current Mayor R.J. Reviczky say the network will save millions that residents would otherwise pay Verizon or Adelphia, and can pay for itself with advertising programs.



DANIEL SOFER

The network in question

The current WLAN covers the heart of downtown, including the beach and the pier, a prominent landmark. If residents go to the trouble and cost of mounting an antenna, the WLAN is accessible to about 30% of this coastal community's population of mainly middle- to upper-middle-class residents, according to Eric Black, president of LA Unplugged, the Hermosa Beach systems integrator that installed the initial network and runs it.

Black used wireless radios and mesh software from Strix Systems to create outdoor nodes. Each node has at least three 11M bit/sec 802.11b radios to handle connections with PCs or laptops fitted with wireless network interface cards. The node has two 54M bit/sec 802.11a radios — one receiving, one sending — to create a wireless backhaul, eliminating the need for Ethernet cabling. All the radios run near the upper power limits set by the FCC to extend their range. Several nodes are mounted on each small rooftop tower.

There are more than 2,000 unique media access control addresses, representing individual clients, that use the network, Black says. The peak throughput is about 5.92M bit/sec, based on a recent test he ran using a movie trailer from www.apple.com. "If you monitor the rate continuously, the typical rate is between 2M and 4M bit/sec," he says.

Today, the WLAN traffic hops via 802.11a wireless bridges to an independent ISP in nearby Long Beach. This, along with two T-1 lines leased for city use, is being replaced with a fiber DS-3 connection from the Wi-Fi Hermosa gateway at the fire station to a fiber trunk owned by Southern California Edison. The city is taking bids from various carriers for Internet access. "We bypassed Verizon and saved thousands" of dollars per month, Keegan says.

But even those savings haven't convinced his fellow councilmen to fund Phase Two of Wi-Fi Hermosa. About $35,000 from the city's general fund paid for the initial rollout of the network, which some councilors saw as a limited pilot test. Operational costs are about $4,500 per month or $54,000 per year, up from an earlier estimate of $24,000, according to a recent report by Burrell. Advertisers on Wi-Fi Hermosa's home page pay monthly fees that total about $1,200 to $1,500 per month.

The extension, estimated by the same report to cost about $126,000, would add more towers and nodes throughout the city, add a DSL connection for backup in case the fiber was cut and set up virtual LANs, which could be tailored for business and residential users.

Residential backers of the wireless network have packed recent council meetings, adding to the debate. But local businesses have been largely silent, and the Chamber of Commerce has not taken a position for or against the wireless network.

Many of the chamber's 350 business members are small and while most have broadband access, they don't tend to exploit it for e-commerce and haven't expressed much desire to let customers tap into it, says Carla Merriman, executive director of the Hermosa Beach Chamber of Commerce. What's more, the cost of switching to wireless isn't cheap. Two chamber members were told it would cost between $5,000 and $10,000 to upgrade their hotel properties to use the public WLAN, Merriman says.

Keegan is convinced that if the network were extended citywide, advertising would become more attractive and advertising revenue would increase to cover operational costs. It also would be possible, he says, to set up arrangements with online e-commerce sites such as Orbitz, which would refund to the city a cut of each plane ticket booked through the Wi-Fi Hermosa link to Orbitz.com.

"I don't think there are any gray areas here," says Deepa Bharath, a reporter for the Torrance, Calif., *Daily Breeze* who's been covering the debate for the past three months. "It's not moved anywhere. People have their minds made up."

And next November, they can act on those convictions. ■

Got great ideas

■ Got a suggestion for a Wider Net story? An offbeat network industry-related topic? A fascinating personality we should profile? Contact Bob Brown with your ideas at bbrown@nww.com.

NetworkWorld

EDITORIAL DIRECTOR: JOHN GALLANT
EDITOR IN CHIEF: JOHN DIX

■ NEWS
EXEGUTIVE EOITOR, NEWS: BOB BROWN
ASSOCIATE NEWS EOITOR: MICHAEL COONEY
ASSOCIATE NEWS EOITOR: PAUL MCNAMARA

■ NET INFRASTRUCTURE
SENIOR EOITOR: JOHN COX (978) 834-0554; Fax: (978) 834-0558
SENIOR EOITOR: TIM GREENE
SENIOR EOITOR: PHIL HOCHMUTH
SENIOR EOITOR: ELLEN MESSMER, (941) 792-1061

■ ENTERPRISE COMPUTING
SENIOR EOITOR: JOHN FONTANA (303) 377-9057; Fax: (303) 377-9059
SENIOR EOITOR: DENI CONNOR (512) 345-3850; Fax: (512) 345-3860
SENIOR EOITOR: JENNIFER MEARS, (608) 836-8490; Fax: (608) 836-8491

■ APPLICATION SERVICES
SENIOR EOITOR: CAROLYN DUFFY MARSAN, (703) 917-8621; Fax: (703) 917-8622
SENIOR EOITOR: ANN BEDNARZ (612) 926-0470
SENIOR EOITOR: DENISE DUBIE
SENIOR EDITOR: CARA GARRETSON, (240) 246-0098

■ SERVICE PROVIDERS
SENIOR EOITOR: DENISE PAPPALARDO, (703) 768-7573
MANAGING EOITOR: JIM DUFFY (716) 6S5-0103

■ NET.WORKER
MANAGING EOITOR: TONI KISTNER, (617) 868-6624

■ COPY OESK/LAYOUT
MANAGING EOITOR: RYAN FRANCIS
COPY GHIEF: BRETT COUGH
COPY EOITOR: MONICA HAMILTON
ASSOGIATE GOPY EOITOR: KYLE CONNORS

■ ART
OESIGN OIREGTOR: TOM NORTON
ART OIRECTOR: BRIAN GAIDRY
SENIOR OESIGNER: STEPHEN SAUER
ASSOGIATE OESIGNER: ERIC ANDERSON

■ FEATURES
FEATURES EOITOR: NEAL WEINBERG
SENIOR MANAGING EOITOR, FEATURES: AMY SCHURR
OPINIONS PAGE EOITOR: SUSAN COLLINS

■ GLEAR GHOICE TESTS
EXECUTIVE EOITOR, TESTING: CHRISTINE BURNS, (609) 683-4432
SENIOR EOITOR, PRODUCT TESTING: KEITH SHAW, (S08) 490-6S27
LAB ALLIANGE PARTNERS: JOEL SNYDER, Opus One; JOHN BASS, Centennial Networking Labs; BARRY NANCE, independent consultant; THOMAS POWELL, PINT; Miercom; THOMAS HENDERSON, ExtremeLabs; TRAVIS BERKLEY, University of Kansas; DAVID NEWMAN, Network Test; CHRISTINE PEREY, Perey Research & Consulting; JEFFREY FRITZ, University of California, San Francisco; JAMES GASKIN, Gaskin Computing Services, MANDY ANDRESS, ArcSec; RODNEY THAYER, Canola & Jones
CONTRIBUTING EOITORS: DANIEL BRIERE, MARK GIBBS, JAMES KOBIELUS, MARK MILLER

■ NETWORK WORLD FUSION
EXECUTIVE EOITOR, ONLINE: ADAM GAFFIN
MANAGING EOITOR: MELISSA SHAW
MANAGING EOITOR, ONLINE NEWS: JEFF CARUSO, (631) 584-5829
ASSOCIATE ONLINE NEWS EDITOR: LINDA LEUNG, (510) 768-2808
MULTIMEOIA EOITOR: JASON MESERVE
SENIOR ONLINE GOPY GHIEF: SHERYL HODGE
SENIOR ONLINE GRAPHIG OESIGNER: ZACH SULLIVAN

■ SIGNATURE SERIES
EOITOR: BETH SCHULTZ, (773) 283-0213; Fax: (773) 283-0214
EXEGUTIVE EOITOR: JULIE BORT, (970) 482-6454
COPY EOITOR: BRETT COUGH

EDITORIAL OPERATIONS MANAGER: CHERYL CRIVELLO
OFFICE MANAGER, EDITORIAL: GLENNA FASOLD
EDITORIAL OFFIGE AOMINISTRATOR: PAT JOSEFEK
MAIN PHONE: (508) 460-3333
E-MAIL: first name_last name@nww.com

Vulnerable
continued from page 12

routing infrastructure — the BGP protocol and the routers themselves — to be its most vulnerable parts. Work continues to improve routing security through the IETF's Routing Protocol Security (RPSec) working group, which has published new documents on generic threats and security requirements for routing protocols, and Open Shortest Path First vulnerabilities within the past six months.

RPSec plans to continue to evaluate and document current and proposed routing security mechanisms. Meanwhile, U.S. CERT under the Department of Homeland Security continues to post vulnerability alerts on Cisco and Juniper routers, in addition to other cyberthreats.

Software bugs also are a problem for Internet hosts and endpoints. Indeed, the majority of worms and other successful cyberattacks are made possible by vulnerabilities in a small number of common operating system services on Internet hosts, according to The SANS Institute, a security training and certification organization that annually publishes a Top 20 Internet security vulnerability list.

"If you want to hurt the network you attack the routers; but if you want to hurt the people using the network, then the operating systems right now are the main attack vector," says Alan Paller, director of research at SANS.

The spread of infamous worms such as Blaster, Slammer and Code Red can be traced directly to exploitation of unpatched vulnerabilities, according to SANS. Attackers scanning the Internet for vulnerable systems count on major corporations not fixing the problems.

But the problems are not theirs to fix, Paller says.

"Vendors have complete responsibility," he says, adding that product vendors and ISPs should work more closely to better secure host operating systems.

The operating system vulnerabilities have minimal effect on the security of the 'Net infrastructure, as Paller noted. However, they serve as the primary attack vehicle for those looking to disrupt specific sites.

With that, SANS publishes patches and workarounds for the Top 20 vulnerabilities. Also, Microsoft continues to work on Windows patch management tools, code to thwart worms and hackers, and acquisitions of anti-virus, anti-spyware and anti-spam companies.

"If I was going to try and arrange a DNS 9/11, it's a very bad target to try and attack because it's so distributed — you'd have to take [the servers] out everywhere."

Paul Mockapetris
Chairman and chief scientist of Nominum and inventor of DNS

Microsoft also has offered to work more closely with governments around the world on detecting and mitigating IT security threats.

Meanwhile, open source developers and vendors continue to develop their own patch management tools.

Internet watchers say the network of networks remains vulnerable to attack but is in better shape than it was two-and-a-half years ago.

"There are a number of things that could have a multi-hour major impact, but I doubt very much that there is anything that would have even as much as a day's impact over any significant chunk of the 'Net," Harvard's Bradner says.

Those operating and securing the Internet insist it's no more vulnerable than any other business-critical infrastructure.

If the 'Net went down, "it would be another disaster, just like many of the natural disasters," IETF's Hartman says. "But business is about managing those risks."

Still, it's a risk that perhaps warrants more continual attention than any other.

"I just think we're putting a lot of eggs into a basket that doesn't have enough control around it," Fidelity's Jarvis says. ■

and then it hits you://

YOU CAN GET 24/7 SUPPORT FOR LINUX

NO MATTER WHERE YOU ARE.

Novell®

find out more at novell.com

©2005 Novell, Inc. All rights reserved. Novell is a registered trademark of Novell, Inc. in the United States and other countries.

EMC²
where information lives

Fr: chained to your desk

To: free to take that vacation

© 2004 EMC Corporation

EMC CLARiiON® CHANGES THE WAY YOU THINK ABOUT STORAGE. Your information and applications will be there when you get back. But some of the hassles of managing them will be gone forever. The new CLARiiON CX series makes your online information safer and gives you simple, powerful management software. Network flexibility for SAN or NAS. Scalable solutions starting below $10,000. To learn more, visit www.EMC.com/backup. Or call 1-866-464-7381.

EMC² VELOCITY² PARTNER

Find an authorized EMC Velocity² Partner at www.EMC.com/velocity.

SAVE $129

NetworkWorld®

Apply for a **FREE** Subscription

($129 value)

- 51 weekly issues
- Expert opinion
- Product tests and reviews
- 6 special issues

Subscribe today at my.nww.com

enter priority code B04A

SAVE $129

FREE

Subscribe today at

my.nww.com

Enter priority code B04A and SAVE $129

NetworkWorld®

Net Infrastructure

■ SECURITY ■ SWITCHING ■ ROUTING
■ VPNS ■ BANDWIDTH MANAGEMENT
■ VOIP ■ WIRELESS LANS

Short Takes

■ SSL VPN vendor **enKoo** has announced two products that enable remote control of network-based PCs and remote access via secure SSL tunnels from the Web browsers of remote machines. The **enKoo Remote Desktop** appliance lets remote users connect to PCs on corporate LANs, and take direct control of the machine's mouse and keyboard. **EnKoo Remote Server** is adding support for accessing Citrix servers and Terminal Services to its remote-access gateway. The server already supported access to e-mail and Web applications. The entry-level price for Remote Desktop and Remote Server is $995.

■ **SMC Networks** last week released two four-port asymmetric DSL2 routers with integrated VoIP gateways aimed at branch-offices users. The company also tacked on wireless LAN connectivity to one of the boxes. The **SMC7904BRA** router combines four ports of 10/100M bit/sec Ethernet with a WAN router and a RJ-11 phone jack for linking to an ADSL link. The **SMC7904WBRA** includes these specifications and an integrated 802.11g WLAN access point feature. Both routers use ADSL2 technology, which provides up to 12M bit/sec of WAN bandwidth for downloading. Pricing for the routers is not available.

■ **Qualys** this week is scheduled to announce the fourth version of its **QualysGuard** vulnerability management service. Version 4.0 adds XML-based application programming interfaces, which can be used to integrate QualysGuard vulnerability assessment information into about two dozen third-party products, including security management consoles, intrusion-detection systems and network management ticketing systems. QualysGuard Version 4.0 is priced ranging from about $1,500 to $17,000 annually.

Force10 crams switch full of Gig E

■ BY PHIL HOCHMUTH

Force10 Networks this week is expected to announce a 90-port Gigabit Ethernet module for its E series chassis switches aimed at data centers with large server clusters.

The module is offered as a way for large companies and research organizations to plug dozens of servers into one switch via Gigabit Ethernet. This can help companies better manage server and switch hardware by plugging servers directly into a backbone device, eliminating multiple switches, the vendor says.

The module offers connectivity for 90 10/100/1000M bit/sec links and is intended for connecting racks of servers. This is the most Gigabit Ethernet connectivity in a single blade among competitive products from Cisco, Enterasys Networks, Extreme Networks and Foundry Networks, experts say. The Force10 blade uses the 380G bit/sec of bandwidth between module slots and the 5T bit/sec switch fabric inside Force10's E1200 and E600 series boxes. Fully loaded, a 14-slot E1200 now can support up to 1,260 Gigabit Ethernet ports that simultaneously can run at full speed, the vendor says.

Force10's 90-port Gigabit Ethernet module might help data centers cut down on hardware without sacrificing speed.

Most vendors offer 48-port Gigabit Ethernet blades as the highest density in a single module. Foundry last year released a 60-port Gigabit Ethernet module, although its BigIron MG8 switch has 40G bit/sec of bandwidth between module slots and the switch fabric.

Force 10's module has 15 telco connection ports, each of which can be split into six Gigabit Ethernet ports via a RJ-45 patch panel. While vendors such as Cisco and Extreme have 96-port telco-connector-based modules, these blades support 10/100M bit/sec connections, and are generally deployed in wiring closets, where many end-user ports are aggregated into one switch chassis.

"It's a heck of a lot of ports," says Zeus Kerravala, an analyst with The Yankee Group. "What they're trying to do is show the scalability of their box. None of the other guys can do 90-Gigabit ports at wire speed in a single blade right now."

It is common for users to deploy telco-based switch modules, which use a patch panel to fan out connections to a greater number of ports that can physically fit on one blade. But these links typically were deployed for end-user connectivity and not on potentially critical server links in a data center.

"There might be a little bit of a stigma" about deploying telco ports for connecting servers in a data center, Kerravala says. But he says carriers have done this for some time and that if deployed with redundancy — two blades with redundant connections to dual-network interface card servers — hardware reliability is probably a non-issue.

The 90-port telco-based Gigabit Ethernet module costs $55,000. ■

Symantec readies anti-spyware products

■ BY ELLEN MESSMER

Symantec this month is scheduled to make spyware protection available as part of its anti-virus software products, joining anti-virus competitors McAfee, Trend Micro and Computer Associates in looking to help users eradicate the problem.

By the end of April, Symantec says it expects to ship AntiVirus Corporate Edition 10.0 with added detection for thousands of types of spyware and adware. A second enterprise product, Symantec Client Security 3.0, which combines anti-virus, a personal firewall and intrusion prevention, also will get spyware protection. A third product out in free beta this week for consumers and small businesses, Norton Internet Security 2005 AntiSpyware Edition, adds spyware eradication to its anti-virus and firewall capabilities. It's expected to ship in June.

The three products use the same anti-virus and anti-spyware signature technologies. The main difference is AntiVirus Corporate Edition and Client Security can be centrally managed by a common console, while the AntiSpyware Edition cannot.

Some customers say they have been waiting to buy anti-spyware software until they see how well — and at what price — the anti-virus providers go into battle against it.

"Spyware, malware and adware is extremely prolific. It's reached alarming levels," says Matthew Fiddler, assistant director for information security at The Hartford Financial Services Group, which uses Symantec products. The Hartford, which began testing anti-spyware software in its labs, so far hasn't found any anti-spyware agent that can protect against everything.

Pricing is another issue.

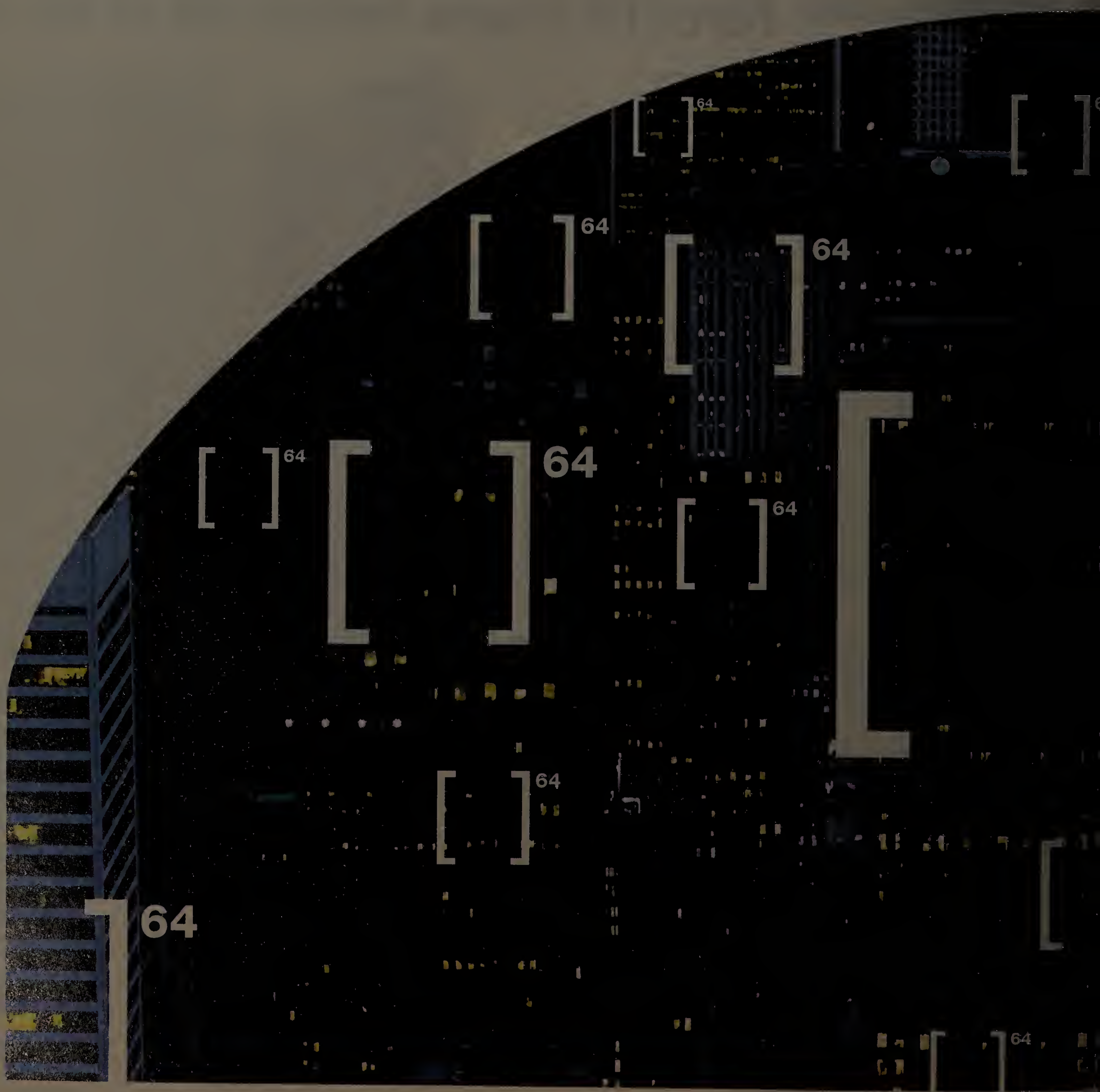
For example, Symantec is charging consumers almost double for spyware protection, though its current anti-virus subscribers are being offered a $30 rebate. Corporate anti-virus customers, which typically do well through volume discounts, will pay far less of a premium — and perhaps nothing additional — for adding spyware protection.

Spyware — the broad and hazy name for thousands of Trojans, system monitors and adware code that might compromise privacy and security — suffers from lacking the neat cataloging that has come to distinguish the many species of viruses and worms.

Symantec says it wants to play a role in establishing common definitions and a way to share spyware samples that will help the industry build comprehensive detection and eradication products that are easy to compare.

"We'll soon announce an independent body similar to the Anti-Phishing Working Group, for spyware," says Kraig Lane, a product manager at Symantec. The new organization will include consumer advocate groups and industry participants. An earlier anti-spyware industry group, called COAST, recently fell apart. ■

©2005 Intel Corporation. Intel, Intel Inside, the Intel Inside logo, and Intel Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. All rights reserved.



The world's most-deployed server platform now supports 64-bit applications. The Intel® Xeon™ processor now works harder for your business than ever. With innovative platform features that enable power-saving options, flexible memory, I/O and storage configurations. And, of course, continued support for all your existing 32-bit applications.

How can Intel Xeon processor–based servers serve you?
intel.com/go/xeon

intel®

Start-up focuses on sharper video

■ BY JASON MESERVE

A videoconferencing start-up is looking to change the way users look at video: LifeSize Communications is set to announce two new endpoints capable of delivering high-definition video, 10 times the resolution of traditional video gear.

LifeSize's new Room and Exec endpoints are capable of delivering up to 1,280-by-720-pixel resolution video with 1 million pixels at 1M bit/sec, while the majority of systems available today only deliver 352-by-288-pixel resolution video (known as full CIF) with 100,000 pixels. At 384K to 512K bit/sec, the typical bit rate for inter-company communications, LifeSize says it delivers resolutions of 720 by 480 pixels — the same as home DVD players.

"The resolution of video calls hasn't changed in 20 years, since the mid-'80s when video went commercial," says Craig Malloy, CEO and founder of LifeSize, and a former senior vice president of Polycom. "Today, you get full CIF video, which is less than half the resolution of broadcast television and one-third that of DVDs. If TV looked like that, you wouldn't watch it."

LifeSize's Room endpoint comes with a custom-built, high-definition pan-tilt-zoom camera, a built-in multiple control unit (MCU) capable of connecting eight participants simultaneously, and LifeSize Phone, a conferencing phone that acts as a speaker and microphone inputs. The phone comes with a 16-microphone array and can be used on its own with VoIP or public-switched telephone networks. It is capable of 22-kHz audio and uses the MPEG-4 AAC codec, the same that Apple iTunes and iPod use. The company also will offer LifeSize Exec, an all-in-one system that includes camera; microphones; speakers; and 17-inch, 16:9 aspect display. It too includes an embedded eight-way MCU.

Both Room and Exec use the H.264 video standard and support both IP (H.323) and ISDN (H.320) calling. Only calls between LifeSize endpoints can take advantage of the higher resolutions. Calls made to competing endpoints from Tandberg, Polycom, VCON and others will drop back to full CIF video.

"High-definition television is a subtle thing," says Andrew Davis, principal analyst at Wainhouse Research. "It makes the video experience much closer to being there. You can see the logo on the shirt and the wrinkle on the guy's face."

The company will roll out a LifeSize Networker, a gateway for bridging users on IP and ISDN networks, and LifeSize Control, a video management suite for scheduling, Outlook integration and software upgrades. Control also will help support non-LifeSize endpoints, Malloy says.

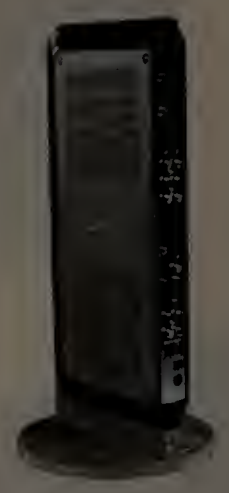
One major feature that LifeSize admittedly doesn't have is a firewall/network address translation traversal product, although one is on the road map. Firewall traversal is a big hurdle remaining in video adoption (see "Vendors target IP video hurdles," www.nwfusion.com, DocFinder: 6737), and competitors Polycom and Tandberg are offering remedies.

LifeSize has garnered $38 million in venture funding and is headed by industry veterans Malloy and Michael Kenoyer, CTO and vice president of engineering. Malloy and Kenoyer co-founded ViaVideo, which Polycom scooped up in 1996 to start its video business. Kenoyer is also a co-founder of V-TEL.

LifeSize plans to roll out its product slate over the course of 2005, with Control available this month, Phone this summer, Room and Networker in the fall, and Exec by year-end. Room will be priced at about $12,000, Exec at about $8,000, Phone starting at about $1,200 (when purchased separately from Room), Networker starting at about $2,000 and Control at about $500 per seat. ■

Make room for LifeSize

Start-up LifeSize Communications is the first new videoconferencing vendor in many years. Its endpoints (LifeSize Room with camera pictured) are capable of delivering high-definition video at resolutions of up to 1,280 by 720 pixels.



Uncertainty reigns in wireless world

■ BY JOHN COX

ORLANDO — You're expecting, or hoping, that wireless and mobile computing for the enterprise will get simpler to figure out.

You're dreaming.

That's the word from the annual Gartner Mobile & Wireless Summit this year in Orlando. The advice from Gartner analysts to several hundred enterprise attendees in session after session boiled down to "Uncertainty reigns. Plan accordingly."

Gartner Fellow Nick Jones encouraged attendees to hammer out innovative wireless contracts with cellular carriers. But then Jones mentioned that it took one British CIO 12 months to get just a straight data contract from his cellular carrier. Apparently, data minus useless bells and whistles was a bit too innovative for the vendor.

Wireless networks are becoming ubiquitous, he said, as 3G cell networks and wireless LANs (WLAN) become more prevalent. But he also said that network latency on cellular data networks will remain a problem for years, potentially crippling a range of real-time applications.

Jones predicted sophisticated applications for the future as prices for cellular radio components, such as those of WLANs, continue to drop. Soon, it will be inexpensive enough to put cellular connectivity into commercial freezers, copying machines and other gear, enabling machine-to-machine telemetry and monitoring.

But many attendees seemed to be still focused on much more basic projects, where ROI is either easily calculated or accepted as a given — simply creating wireless access to data, or turning paper business processes into electronic wireless transactions.

Acuity, a Sheboygan, Wis., insurer, is evaluating how to give field-claims adjusters wireless access to corporate applications, possibly with a laptop fitted with a cellular network interface card, said Tina Pokrzywinski, director of IS. "We're due for a technology upgrade," she said. "And our CIO says, 'Wireless is coming, and we need to be ready.'"

Two managers from a Midwest manufacturer, who asked not to be identified, are researching options for creating a mobile-salesforce automation application.

"Our salespeople want to finish off one call report on the way to their next customer, rather than waiting until the end of the day and working late to do it," said one of them, who manages e-business systems for the company. "We're trying to recapture all that idle time and make them more productive."

"What we're finding is that nothing is 100% ready for prime time," his colleague said.

Wireless security remains a major issue for attendees, and Gartner analysts were not encouraging. Gartner Vice President John Pescatore ran through a list of supply-chain activities, ranging from R&D and CRM to marketing and shopping, all of which face new vulnerabilities as mobile computing makes it easier for sensitive customer, personal and corporate data to end up on unsecure smart phones, PDAs, laptops and MP3 players.

ExxonMobil Exploration, based in Dallas, is authenticating the growing numbers of mobile and wireless clients via the public-key infrastructure (PKI) and certificate authority implemented globally a few years ago.

Originally, PKI was deployed to enable every company employee to be authenticated to a network via a smart card, said Ryan Jarvis, a manager of the company's upstream technical computing group. "The smart cards authenticate the users; PKI lets us authenticate the machines," he said.

"We get people who go home and play with devices they got for Christmas, and they want to bring these onto our network," he said. With PKI, "we can say, 'You're an ExxonMobil machine, and you're not.'"

Don't expect the surging numbers of client devices, with the bewildering choices of operating systems and application frameworks such as Java2Micro Edition and Microsoft .Net, to moderate any time soon, warned Gartner Vice President Ken Dulaney. This year alone, he says he expects at least 80 new cell phones to debut offering cellular and 802.11b wireless connectivity.

"Device convergence will not happen," he told a packed afternoon session. "Proliferation will just get worse."

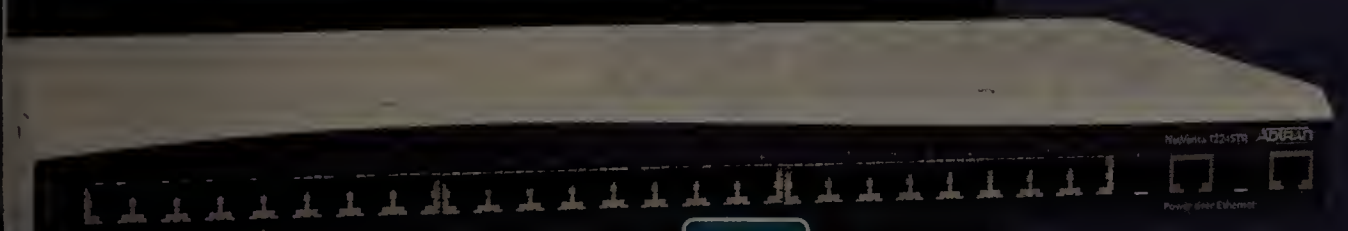
So will the ability for these increasingly capable devices, and wireless connectivity, to circumvent IT control. "The technology available for users to get around IT is really breathtaking," he said.

One IT manager for a retailer with stores in six states said wireless is creating huge liability risks if it makes personal customer data potentially more vulnerable.

"I want to be able to go to any of our stores in those six states, open my laptop and jump on my network," he said. "But I can't let any bad guys do the same thing.

"If [wireless] security gets to the point where it's not 'in your face,' then it's probably not working," he said. ■

The right technology (at the right price).



ADTRAN PoE 802.3af Power over Ethernet

NetVanta 1224R/1224STR Series
Network-in-a-Box with
Switch/Router/Firewall/VPN/DSU/CSU

New!

NetVanta 1224/1224ST Series
Managed Fast Ethernet and
Powered Ethernet Switches

NetVanta 1524ST
Managed Gigabit Ethernet Switch

NetVanta 340
Business-class ADSL2+ Router

NetVanta 3200
Modular 2xT1/ADSL2+ Branch Office
Routers with Firewall/VPN/Voice/Dial Backup

NetVanta 3205/3305/4305
Modular 2xT1/3xT1/8xT1 Routers with
Firewall/VPN/Voice/Dial Backup

NetVanta 5305
Modular 2xT3 Router with Firewall/VPN

NetVanta 2050/2054/2100
Home Office/Small Office VPN Gateways
with Firewall/Multi-Port Switch

NetVanta 2300/2400
Medium to Large Office VPN
Gateways with Firewall

NetVanta® Switches, Routers, and VPN Solutions.

Is voice and data networking costing you more than it should? You no longer have to pay premium prices for brand name gear to perform customary internetworking tasks. With the ***NetVanta Series*** from ADTRAN®, you can implement the ***exact internetworking functionality*** you need, at a cost that's often ***50% less*** than competing brand name solutions. Choose from ***switching, routing, and VPN*** platforms. Modular chassis and ***deep product lines*** let you pick and choose just the right solution for ***any application***—data, voice, ***VoIP, Internet***, backup, and management—across networks ranging from 56 kbps to GigE. Every solution is backed by a ***100% satisfaction guarantee*** from ADTRAN, unlimited telephone technical support (before and after the sale), ***free firmware upgrades***, and a full 5-year warranty.

Lower network costs without compromising quality, performance, or support — with NetVanta.

VoIP Ready

Why pay more (when you don't have to)?

Compare now! Receive a free white paper on reducing total cost of ownership.
www.adtran.com/rightprice

Have a question about network design? How to implement VoIP in your network? Our network engineers are standing by.

800 597 9602 Technical Questions
877 280 8416 Where to Buy

TOLLY Up to Spec CERTIFIED

5

Win an iPod mini!
N+I
Booth 2324

The Network Access Company ADTRAN®

Copyright © 2005 ADTRAN Inc. All rights reserved. ADTRAN and NetVanta are registered trademarks of ADTRAN, Inc. iPod is a registered trademark of Apple Computer, Inc. Five-year warranty applies in North America and Europe. EN89C032805NW

Special Focus

WI-FI NETWORKS: Gaining quality.

Standard set to boost wireless QoS

■ BY TIM GREENE

A standard to define QoS in Wi-Fi networks is coming soon, but even before it is finalized users can expect QoS improvements from vendors that have implemented their own performance-enhancing technologies.

Wireless hardware vendor Colubris Networks says a pending software upgrade will improve its monitoring of call quality, so perceived bad quality can trigger automatic adjustments to a wireless network or alert administrators to deal with problems it has identified elsewhere on a connection.

Aruba Wireless Networks will support an informal QoS standard created by the Wi-Fi Alliance that is already supported by more than a dozen other wireless vendors. Similarly, Trapeze Networks will support the same Wireless Multimedia (WMM) specification with its next software release, due within 90 days.

The flurry of activity surrounding Wi-Fi QoS is mainly due to the growing popularity of voice over Wi-Fi (VoWi-Fi) and the demand that phone calls be reliable and intelligible, says Ellen Daley, an analyst with Forrester Research. A host of vendors, including 3Com, Broadcom, Cisco, Linksys, Conexant, D-Link Systems, HP, IBM, Intel, NEC and Netgear, already have certified their gear is WMM-compliant.

WMM is a subset of the IEEE RFC known as 802.11e, which vendors expect will be approved this year. WMM was created to promote use of QoS that would be interoperable among multivendor Wi-Fi gear, she says. "That means businesses can do voice over wireless pretty respectably today. They may need to upgrade when the standard comes out if they want to be standards-compliant," Daley says.

But for most users, the life cycle of wireless gear is short enough that just about the time wireless gear bought today is ready for replacement, the 802.11e gear should be ready to buy, says Craig Mathias, a principal at Farpoint Group. In the meantime, most Wi-Fi customers are getting by with single-vendor deployments of QoS-enabled devices or deployments of multiple vendors' gear whose QoS schemes have proven interoperable, he says.

The overriding challenge for QoS is that Wi-Fi is a shared medium, much as Ethernet was in the days before switching. There is just so much bandwidth and client devices have to share.

Three years ago, Bob Longhini was evaluating BreezeCom VoWi-Fi gear for door and window maker Kolbe & Kolbe, but pulled the plug on the project because of QoS issues. "We had echo and breakup in the calls, especially if there was activity from handhelds and laptop computers," says Longhini, who now is evaluating VoWi-Fi for his new employer, Jennie-O Turkey Store, a billion dollar subsidiary of Hormel.

Only workers with desperate need for mobile phones liked the early equipment, he says. "They really saw the benefit of having the phone on their hip even if they ran into quality problems," Longhini says. But things have greatly improved with a clear road map being set for QoS and many vendors already implementing early versions of the standards-bound technology.

Ideally, client devices — in the case of VoWi-Fi that means phones — would announce their bandwidth requirements and the wireless network would take steps to accommodate them, if possible. In its WMM implementation, Cisco's wireless gear (formerly Airespace) checks whether an access point in range of the phone has enough free bandwidth to accommodate the call, says Kathy Small, Cisco's marketing manager for wireless and mobility. WMM then can offer four levels of service.

WMM addresses how clients and access points communicate what they need and what they can provide, respectively, but not how devices decide whether to accept an available connection, says Partha Narasimhan, wireless architect for Aruba. Even with WMM, that is left up to individual vendors to implement, he says.

Once a phone is accepted by an access point, algorithms determine when each device connected to a single access point gets to send, with top priority voice traffic getting to send more often, says Roger Sands, vice president of enterprise development for Colubris. These algorithms were created to deal with collisions and retransmissions on Wi-Fi networks but have been fine-tuned to give voice the edge over other applications. Properly adjusting these algorithms in Colubris gear shaves at least 20 microsec off a packet's wait time, according to Colubris engineers.

WMM also calls for phones to tag voice packets so access points and wireless switches can treat inbound packets with priority and drop them onto the appropriate virtual LAN in wired networks to which access points are connected. Many companies create separate VLANs just for voice to ensure QoS and boost security.

Similarly, wireless switches mark outbound voice packets for top priority "to make sure they don't sit in the access point waiting for data packets," Sands says.

Once VoWi-Fi users make calls, they likely will move around, forcing the wireless network to hand off the calls from access point to access point. "Roaming is critical," Cisco's Small says.

"But with QoS plus mobility, you have an even bigger problem," Aruba's Narasimhan says. Both the handsets and the access points have to seek the next access point for the caller to connect to and figure out if it has the bandwidth to accept the call, he says.

A separate proposal called 802.11r is in the works to deal with roaming, where the key problems are maintaining the security state and the QoS context for the call without forcing the handset to carry out a full negotiation with the next access point, he says.

Enabling handoffs with QoS might call for each access point to reserve some bandwidth to deal with handoffs of ongoing calls. This bandwidth buffer would be adjustable and set by network executives depending on how much their users roam.

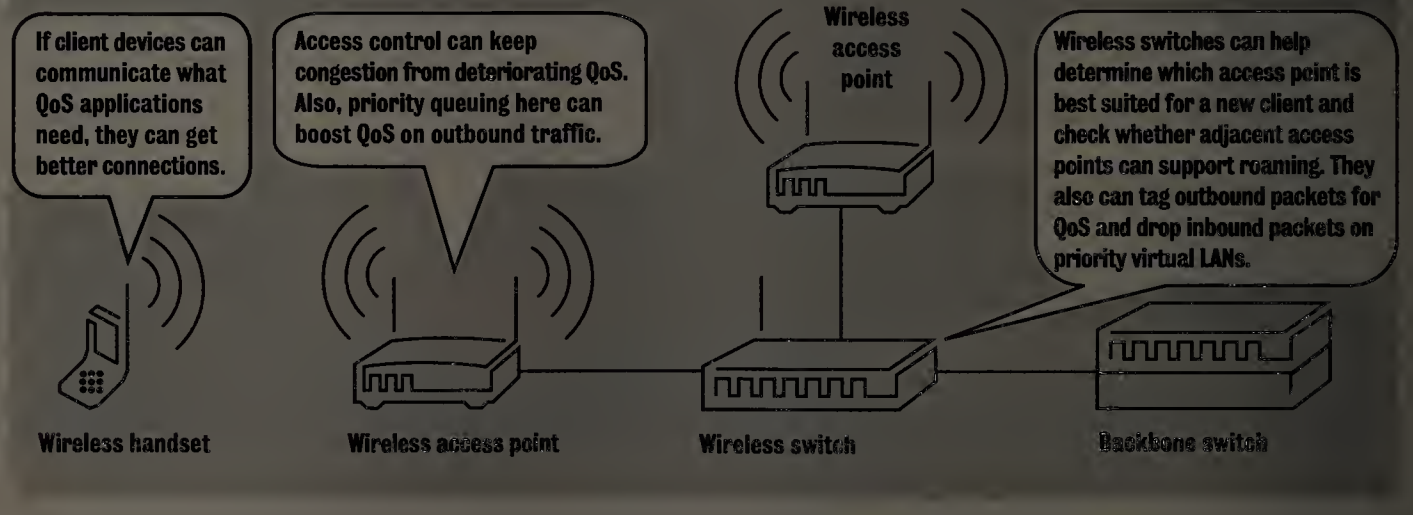
Handoffs are unnecessary in the office segment of the Aruba wireless LAN at Commercial Alcohols, an alcohol distributor in Brampton, Ontario, says Chris Thomas, the company's IT director. But in the warehouse, where managers move around quite a bit, smooth handoffs are a requirement. So a small buffer or none at all might be sufficient for the office segment, while a significant percentage of total bandwidth might be required in the warehouse.

As 802.11e and 802.11r near completion, Spectralink, the vendor that created the predominant non-standard wireless QoS mechanism, is planning to abandon its earlier technology and adopt standards. Spectralink Voice Priority (SVP) was adopted by the major VoWi-Fi vendors and now is being replaced by WMM. "The SVP approach was great and got us where we are today and is the reason we have voice over Wi-Fi at all today," says Ben Guderian, director of marketing strategy for the company. "But it's served its purpose."

The question remains whether customers will want gear that is fully compliant with 802.11e or whether WMM supports stringent enough QoS to meet business needs. "The goal may become a balance between QoS and complexity," says Bruce Van Nice, vice president of marketing for Trapeze. "Users tend to balance toward the pragmatic." ■

Where QoS can help Wi-Fi

QoS standards and proprietary offerings try to address how Wi-Fi network components can support QoS for applications such as voice and video.



Oracle Database

World's #1 Database
Now
For Small Business

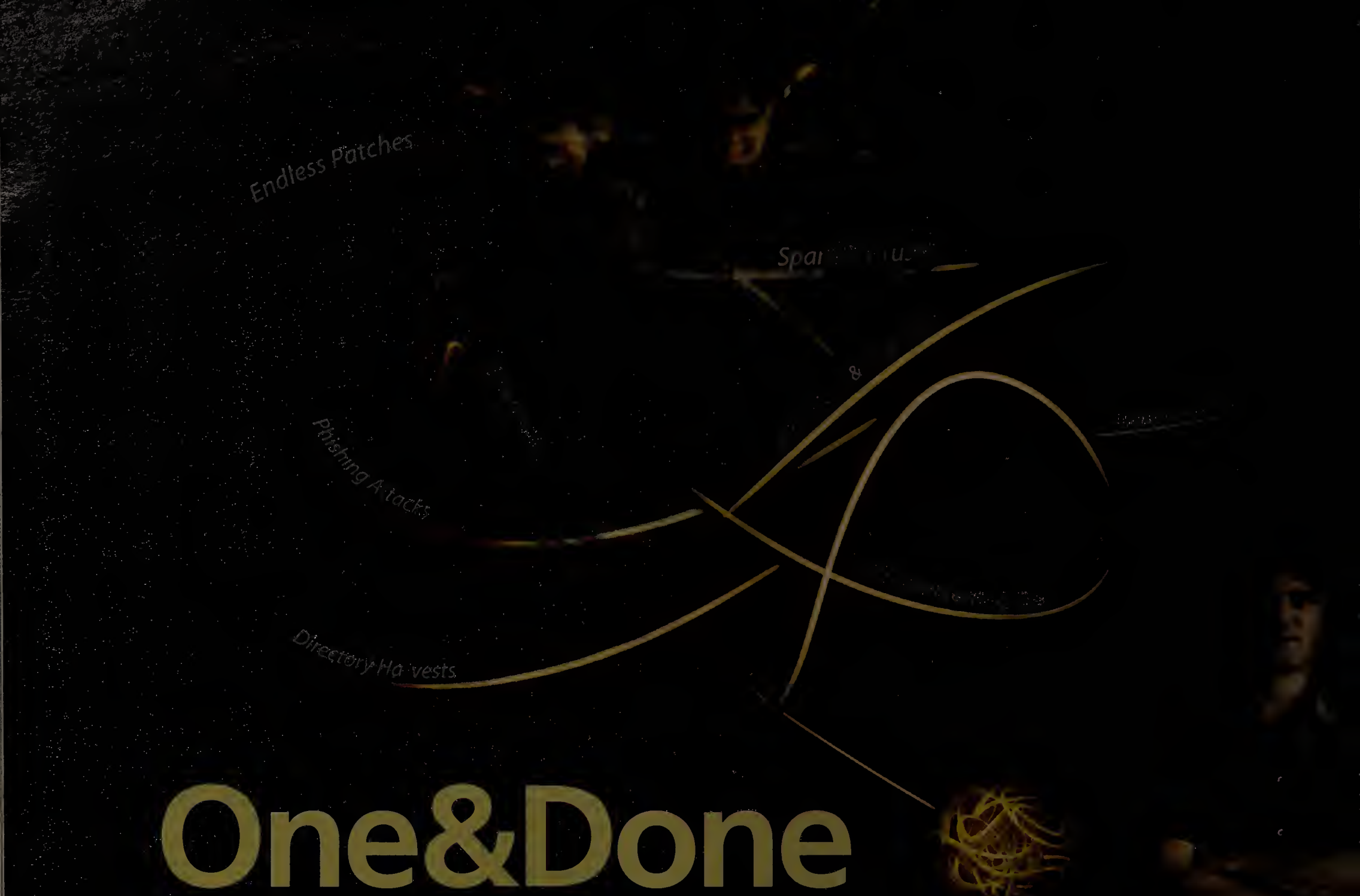
Easy to use. Easy to manage. Easy to buy at Dell.
Only $149 per user.

ORACLE®

dell.com/database
or call 1.888.889.3982

Terms, conditions and limitations apply. Pricing, specifications, availability and terms of offers may change without notice. Taxes, fees and shipping charges extra, vary and are not subject to discount. U.S. Dell Small Business new purchases only. Dell cannot be responsible for pricing or other errors. Oracle Database Standard Edition One is available with Named User Plus licensing at $149 per user with a minimum of five users or $4995 per processor. Licensing of Oracle Standard Edition One is permitted only on servers that have a maximum capacity of 2 CPUs per server.
For more information, visit oracle.com/standardedition

Copyright © 2004, Oracle. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.



One&Done

One company.
One appliance.
One step closer to easier messaging...

For nearly 10 years, Mirapoint appliances have been the backbone for more than 60 million mailboxes for customers like Ford, STMicroelectronics, RSA Security, British Telecom, China Telecom, University of Georgia and CalPoly.

With powerful spam and virus edge-blocking technology, ultra-reliable email, advanced messaging & mobility features, plus feature-rich collaboration including group calendaring and shared folders, we deliver the complete messaging lifecycle. We know messaging is complex, and Mirapoint is helping to ease the strain on IT by delivering modular, standards-based appliances for email and security.

Whether you need a complete messaging solution or better security protection, Mirapoint delivers.

MIRAPOINT®
For You, The Messaging Experts

mirapoint.com/done

Enterprise Computing

■ WINDOWS ■ LINUX ■ SERVERS ■ UNIX
■ STORAGE ■ GRID/UTILITY ■ MOBILE COMPUTING

Short Takes

■ Web content acceleration company **FineGround** is expanding into **remote office backup and recovery** with a new appliance that performs wide-area file services for Windows environments. The Velocity-FS box sits in the data center where it collects changes to files made in a branch office. The idea is to take on the job of doing backups that rarely get done in branch offices, which often lack IT administrators. Velocity-FS is compatible with all major storage and file systems. It supports Microsoft Active Directory and rights management systems, Distributed File System capabilities, and desktops such as Windows XP or later and Mac OS X. The appliance, which will be available at the end of the second quarter, starts at $20,000.

■ **ADIC** last week launched a version of its disk-based back-up system that boasts 2T to 5T bytes of storage capacity. The **Pathlight VX 450's** integrated tape support lets IT staff back up data to tape for archival purposes without involving the media server. The VX 450, which can be divided into as many as 20 virtual drives, supports ADIC Scalar libraries and uses EMC Clariion ATA drives. The rack-mountable system uses 2G bit/sec Fibre Channel to attach to a storage-area network. It starts at $60,500.

■ **Azul Systems,** a start-up that is promising computing power on demand for Java-based applications, this week is expected to begin shipping its first products. The **Azul Compute Appliance** handles Java processing workloads on behalf of traditional application servers. The Azul Compute Appliance 960, for test and development environments, has 96-processor cores and 32G bytes of memory and costs $89,000. The Compute Appliance 1920 comes with 192 processor cores and 64G bytes of memory and costs $199,000; and the Compute Appliance 3840 comes with 384 processor cores and 128G bytes of memory for $499,000, or 256G bytes of memory for $799,000.

Software tames thin-client setups

■ BY JOHN FONTANA

TriCerat last week released a suite of tools designed to help users manage their server-based computing deployments.

The company's Simplify Suite is a collection of four tools for managing user profiles, locking down privileges, managing resources such as memory and CPU usage, and supporting printing features regardless of installed drivers. The tools, which are available through a single administrative console, load on to a Windows 2000 or 2003 server that is supporting server-based computing and thin clients either through Windows Terminal Services or Citrix MetaFrame.

"This is what administrators want," says Bill Heldman, an analyst with Enterprise Management Associates. "If administrators can deploy high-quality application virtualization they would adopt [server-based computing] more quickly."

He says TriCerat, along with competitors such as AppSense, RTO Software and Aurema, are rounding the rough edges users find when they deploy server-based computing, especially in the area of printing.

"Printing issues are a huge turnoff," Heldman says. "If I have to support telecommuters and they can't print, companies say they are not going to do that."

Simplify Printing, which incorporates TriCerat's TriMeta driverless printing technology, allows end users to print from any applications, regardless of the drivers installed on their machines. Typically, administrators have to configure printing on a user-by-user basis and ensure that the drivers on the server-based system match those on the end-user desktop. Simplify Printing configures all the printing capabilities on the fly when the user connects to the application.

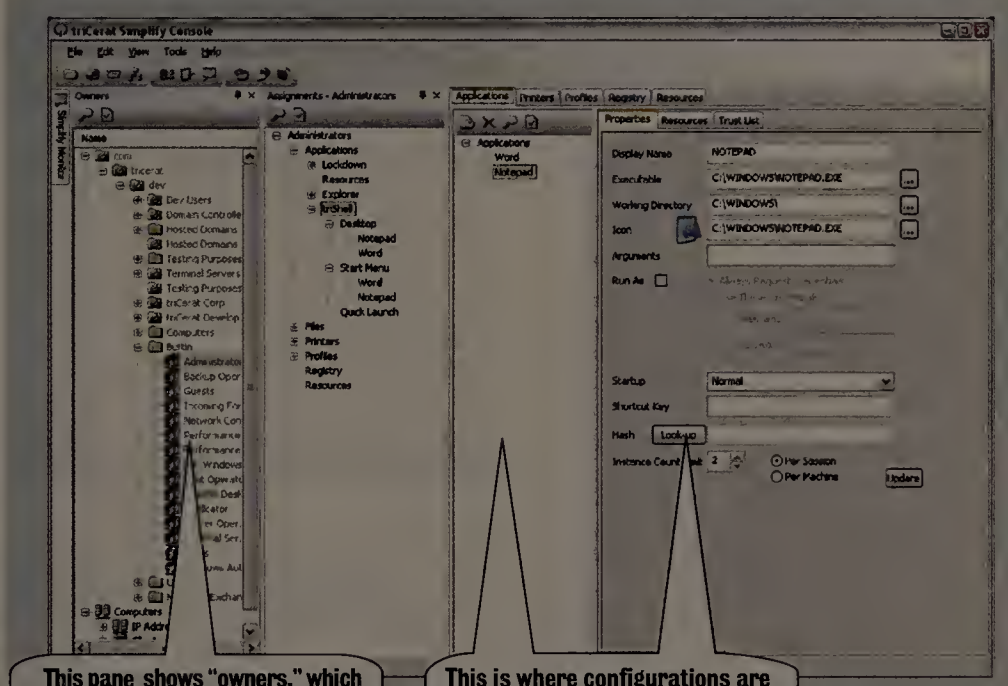
The suite also contains a tool called Simplify Lockdown that allows administrators to limit privileges of end users such as running unauthorized applications, tools or scripts.

The limitations, which can be applied at various levels including IP address,

See TriCerat, page 27

Central view

The tools in TriCerat's Simplify Suite for managing server-based computing environments are all exposed through a single interface.



Softricity touts Web-based app access

■ BY JOHN COX

New software from Softricity will let end users access their desktop applications from any computer with a Web browser.

Softricity's ZeroTouch software is designed to turn more of the work of deploying desktop and server applications into an automated workflow managed by end users. That, the company says, eases the burden on network help desks and IT staff.

With ZeroTouch installed on a server, users connect to a secure Web site or a Web portal from vendors such as Plumtree. Once authenticated, users get the ZeroTouch Web page, which displays icons of all their authorized applications, wherever they're installed.

Clicking an icon launches the application, and at this point ZeroTouch relies on Softricity's SoftGrid client/server software. SoftGrid "virtualizes" an application (see www.nwfusion.com, DocFinders: 6732 and 6733). In effect, it translates the application code into a package of files, stored on the SoftGrid server along with Softricity's virtual run-time environment. When a user clicks on an application icon, this package downloads to the PC or to another server. Instead of being installed on the computer, the application files run in a protected virtual space, similar to that created by a Java virtual machine.

Softricity is one of a small group of vendors that are virtualizing applications. The general idea is the same: separate and insulate applications from the underlying operating system and hardware to simplify deployment, operations and management. The vendors take different approaches, some focusing on server-based applications, some like Softricity on desktop programs. Other vendors include Datasynapse, with its GridServer, and Trigence with its Trigence Application Environment.

Americo Life Insurance of Kansas City, Mo., is a Softricity SoftGrid user, and is

See Softricity, page 27

poweredbycisco.

officepark

Customer preferences, billings, account numbers—in short,
everything to get the job done—now available in the comfort of home.
In real time. In real terms. Cisco IP Communications brings together
voice, video and data to transform homes into call centers,
so employees don't have to be at work, to be at work.
Learn how Cisco is helping change business at
cisco.com/poweredby.

Cisco Systems

productivity. powered by

WIRED WINDOWS
Dave Kearns

Compliance: A horse is a horse

One of the hottest topics over the past year is "compliance auditing." Regulations from the Health Insurance Portability and Accountability Act to the Sarbanes-Oxley Act require that computer access to data not only be tightly controlled but also heavily monitored, logged and audited. Some regulations require auditing all users and resources and being able to tell — at any point in time — which objects could possible access which other objects and why they should be able to.

This is a far cry from the typical forensic auditing that network professionals did just a few years ago, when audit logs were really only read after a problem had occurred in an attempt to determine who (or what) might have caused the situation. Still, there also have been major advances in these security-monitoring functions.

Let's say there's a very up-to-date horse ranch, with sensors all over the barns wirelessly connected to the ranch network. Constant monitoring of comings and goings of horses and cowboys is logged. Access to individual stalls is controlled with proximity cards, and a verifiable record of who can access which horses is always available.

One morning, it's discovered that the barn door is open and all the horses are missing.

Old-style audit logging would require that we now sit down and read through the logs to discover who was (probably) the last cowboy to leave the barn. "Probably," because if that cowboy didn't lock the door, then there's no record of him leaving. We need to match up all entrances and exits to see where there was an entrance (logon) without a corresponding exit (logout). But the horses are still gone.

If the rancher has good regulatory compliance auditing tools, he could query the command console to see who had access to the barn — and to each horse's stall — during the hours that the security breach might have taken place. He can show the federal investigators whether he was in compliance with all regulations regarding horses, barns and data security. But the horses are still gone.

An up-to-date ranch network armed with sensors, detectors and rules would have noted that the barn doors were unlocked after the time set for them to be locked. It would have noticed horses out of their stalls at a time they shouldn't be. It would have noted a human presence when none had logged on. And it would have responded by locking the door before the horses got out.

What about your company's "horses"? Can you stop them from getting away?

Kearns, a former network administrator, is a freelance writer and consultant in Silicon Valley. He can be reached at wired@vquill.com.

Tip of the Week

If you're interested in locking the barn, automatically, before the horses get out, you might want to look at the partnership between security vendor **Corestreet** and **Assa Abloy,** a leader in lock technology.

Softricity
continued from page 25

about to start beta-testing ZeroTouch as part of its move to a corporate Web portal based on Plumtree's software. It plans to phase out its Citrix server farm, virtualize its desktop applications with SoftGrid, and access them through ZeroTouch.

"ZeroTouch adds a new layer to SoftGrid," says Kimberly Peine, director of emerging technology and architecture for Americo. "I can now let a department manager give her people the applications they need, as they need them, without involving IT. I can tell her, 'you have five licenses for Visio [a Microsoft drawing program], and you can decide who gets to run them.'"

If the manager authorizes specific users, they simply click on the "Manage My Applications" button on the lower right of the ZeroTouch Webpage. On the new page, users see the additional applications, including in this case, Visio. Another mouse click on the "Activate" button, triggers ZeroTouch to assign the application to the user, who has immediate access to it.

From an IT viewpoint "we just leave the PC alone," Peine says.

Peine says she also likes the reporting feature that's part of ZeroTouch. Both she and the department can access Web-based reports on a range of usage data such as who uses what application when, and for how long.

ZeroTouch is scheduled to be available by July. Pricing will be announced at that time. ■

Microsoft storage tool hits the beta stage

■ BY DENI CONNOR

PHOENIX — Microsoft last week announced that its disk-based backup and instant-recovery software is now available for beta testing.

Introduced last September as Data Protection Server, the product has been renamed Data Protection Manager. Microsoft says the product, which is designed to back up as many as eight servers, will let IT administrators continuously back up the Windows NT file system and recover data from any point in time. The company, which aired its latest plans at Storage Networking World last week in Phoenix, says it has back-up support for Microsoft Exchange and SQL Server in the works.

Data Protection Manager works with Microsoft's Active Directory, Windows Server 2003 and Windows Storage Server 2003. Users of Dell, EMC or HP network-attached storage appliances that use Windows Storage Server 2003 also will be able to use Data Protection Manager. It will work with Microsoft's System Center software.

IT administrators who download the beta software will be able to upgrade to the final product when it ships, most likely in the third quarter. Pricing for completed product has not been announced. ■

TriCerat
continued from page 25

machines names, domain or user group, and not only determine what an end user can do but what end users see on their screens.

"The moment you install these tools, the only thing users have is access to log off. Administrators have to build up from there," says John Byrne, president and CEO of TriCerat.

The final two tools in the suite are Simplify Profiles and Simplify Resources. Simplify Profiles lets administrators push user profiles down to a desktop each time an end user logs on. The profiles control the entire end user session, including registry key settings and names of drives. The Simplify Resources tool controls the way Windows allocates CPU and memory to ensure no one application can cripple the performance of the server it is running on.

The Simplify Suite is priced at $3,000 per server. ■

Cisco™ Powered

when you decide on the service, this logo will help you decide on a provider.

Make sure you get the latest in network services by looking for the Cisco Powered logo. From managed business voice to managed security and virtual private networks, this logo means the service is delivered over a network built end-to-end with Cisco equipment—which meets the highest standards for performance and reliability.

To find a Cisco-recommended service provider or to download the *Cisco Guide to Buying Managed Network Services,* go to cisco.com/go/cpnnow1.

Cisco Systems

BRAVO

With lightning speed and brilliant color, no wonder the Xerox Phaser® 8400 printer is getting rave reviews. And starting at just $999, it's cause for celebration. Xerox Color. It makes business sense.

What does $999 buy you? Quite a bit, when you're talking about the Phaser 8400. It prints vivid color plus black and white at the same incredible speed—24 pages per minute. So it's no surprise that it's winning all kinds of industry recognition. Like PC World's Best Buy Award for Color Laser Printers, as

well as Buyer's Laboratory's Pick of the Year for Outstanding Critical Color Printer. Not to mention Better Buys for Business's 2004 Hot Pick Award. To learn more about our full line of Xerox network printers, digital copiers and multifunction systems, call or visit our website today. Champagne, anyone?

PC WORLD Best Buy

HOT PICK 2004 Better Buys for Business

XEROX®

xerox.com/office/winning8400
1-877-362-6567 ext. 1977

Technology | Document Management | Consulting Services

©2005 XEROX CORPORATION. All rights reserved. XEROX®, Phaser® and Xerox Color. It makes business sense are trademarks of XEROX CORPORATION in the United States and/or other countries.

Application Services

■ CRM ■ MESSAGING/COLLABORATION ■ WEB SERVICES
■ ERP ■ E-COM ■ NETWORK AND SYSTEMS MANAGEMENT

Start-up to create open source harmony

■ BY JENNIFER MEARS

A start-up headed by former Marimba CEO Kim Polese is hoping to be the one-stop-shop that companies turn to as they expand the use of open source applications in their data centers.

Called SpikeSource, the company was founded in 2003 to test and certify stacks — or integrated packages — of open source software and then provide support and maintenance for them. Earlier this month, SpikeSource announced the general availability of its Core Stack, which includes seven preconfigured packages that integrate more than 50 open source components on six operating systems — including Linux and Windows — in six programming languages.

"Our focus is to make open source safe for the enterprise," Polese says. "We're doing that through solving one of the biggest problems that has emerged in using open source in production environments: interoperability. ... What's really missing [in open source] is that centralized integration, or productization — what we see in proprietary software."

SpikeSource automates the time-consuming task of ensuring that the hundreds of different combinations of software components — both open source and proprietary — work together. Today, most companies do this manually.

"We're getting fan mail from companies saying, 'What used to take me days now takes me minutes,'" Polese says.

SpikeSource uses a "testing harness" that was two years in the making to test across the possible combinations of software components, operating systems and language run times. The company runs more than 22,000 tests each day across the stacks to identify interoperability issues and apply appropriate fixes, Polese says.

The Core Stack is free and can be downloaded and installed from www.spikesource.com. The company also offers four levels of support, each of which includes an update service. Basic Installation Support is based on 30 days of assistance and includes technical support installing and configuring open source components, priced at $795 per year; SpikeSource Silver Support, which adds incident-based support with a one-business-day response time, is priced at $10,000 per year; and SpikeSource Gold Support, which offers a four-hour response time, 24/7 phone support and is aimed at mission-critical deployments, is priced at $25,000 per year.

Companies in growing numbers are looking beyond Linux to bring in open source versions of middleware such as application servers and databases. The trouble they often face is that integrating the middleware pieces can be tricky, not only because of interoperability issues, but also because of questions around licensing and intellec-

SpikeSource, page 30

PROFILE: SPIKESOURCE

Location:	Redwood City, Calif.
Founded:	April 2003 by Murugan Pal, former CTO of Asera (acquired by Web services firm SEEC in 2003), and Ray Lane, partner at venture capital firm Kleiner Perkins Caufield & Byers; former Oracle COO.
Employees:	More than 40 employees in the U.S., India and the U.K.
Management team:	Kim Polese, CEO; Murugan Pal, CTO; and Nick Halsey, vice president of sales and marketing
Primary services:	Seven preconfigured software stacks incorporating 63 open source components on six platform languages: Java, PHP, Python, Perl, C and C++. The company also provides update services, technical support, management tools and other services associated with the stacks.
Funding:	Funded by KPCB, Intel and Fidelity Ventures. Did not disclose specific finances.
Customers:	Targets financial and government verticals; customers include investment bank Dresdner Kleinwort Wasserstein.
Competition:	SourceLabs, GroundWork, Gluecode and OpenLogic

Short Takes

■ **SAP** is offering a helping hand to companies that outsource administrative processes with the launch of a new support program. As part of the business process-outsourcing program, called BPO Services Powered by SAP, the company will help set up and operate BPO delivery platforms in cooperation with service providers, including Affiliated Computer Services, ADP, Electronic Data Systems and LogicaCMG PLC. SAP's services-oriented architecture, provided through its NetWeaver application and integration platform, is developed to make it easier for companies to move non-core business processes outside the company, while retaining control of information and workflows in a tightly integrated way, the company said.

■ E-mail security gateway maker **IronPort** last week announced that it has struck a deal for e-mail performance management company **Return Path** to take over its Bonded Sender whitelist service. Return Path now is responsible for the operations, marketing and future enhancements of Bonded Sender, while IronPort will continue to feed Return Path the back-end data it needs for the service, says IronPort CEO Scott Weiss. The terms of the deal remain undisclosed. Bonded Sender is a whitelist service under which companies that send legitimate e-mail post a bond ensuring their messages are wanted, and in exchange are not flagged as potential spam in the recipient's anti-spam filter. If a complaint is filed against a bonded sender, a fee is debited from that company's posted bond. Web site certification company Truste provides oversight and dispute resolution for the service.

Software indicates when to discard information

■ BY ANN BEDNARZ

Start-up PSS Systems this week is expected to unveil software designed to help companies automate decisions about which documents need to be saved and which can be tossed.

The company's Atlas Information Policy Management (Atlas IPM) suite looks to help companies create and manage policies for document retention, disposal, preservation and production. Once a company configures its policies, Atlas IPM enforces those policies across disparate data sources, including files stored on PCs, file servers and in data repositories.

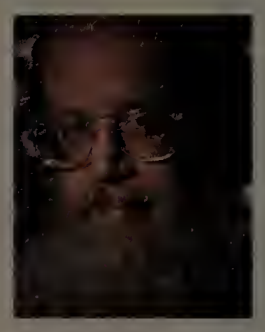
Atlas IPM can help companies reduce their document discovery and storage costs, and improve user productivity, says Deidre Paknad, president of PSS Systems, which was founded in 2001 and backed by $30 million in venture funding. It retains only a single instance of each document and disposes of unnecessary versions or records that have reached their end-of-life stage. On the legal front, the software is designed to help companies more easily find the documents they need to produce.

Companies often have retention policies, but they aren't always uniformly enforced across distributed sites. At the same time, companies store massive amounts of information that don't need to be preserved — which can complicate electronic discovery efforts, says Paknad, who founded CRM vendor CoVia Technologies in 1996 and most recently was a vice president at regulatory compliance software maker Certus.

These days, information policy management software that specifies how and where to retain documents is gaining interest among companies that face compliance with regulations such as the

See PSS Systems, page 30

'NET INSIDER
Scott Bradner



A target in your pocket

This is not just another column on the evils of radio frequency identification, even though it starts out looking like one. This is actually about decision-making.

After a series of closed meetings, the U.N.-sponsored International Civil Aviation Organization developed an international standard for electronic passports. The standard specifies a passport with an embedded RFID-like electronic chip. Unlike the RFID chips I have recently written about (see www.nwfusion.com, DocFinders: 6728 and 6729), which basically contain a unique ID, the chip in the passport will be able to store all sorts of information (eventually up to 512K bytes). The initial information set includes name, date and birthplace, a digital photo and, I expect, the country that issued the passport. The U.S. and a number of other countries are in the process of adopting the standard. As with other RFID chips, the information in the passport chip will be able to be read without the reader having to be in actual contact with the passport. Also, as with other RFID proposals, quite a few people have expressed considerable concern over this remote reading ability, particularly because the data will not be encrypted. The American Civil Liberties Union (ACLU) and Electronic Frontier Foundation both provided comments to the U.S. State Department on the proposed electronic passport. Their comments and backup material are online at DocFinders: 6738 and 6739. Do not read this information if you want to continue to think that the U.S. government wants to protect your safety.

One ACLU document uses information that it obtained under the Freedom of Information Act to detail how the U.S. government repeatedly argued against adding safeguards to the standard, such as encrypting the data or using a device with physical contacts rather than wireless chips, when such safeguards were proposed by other countries. The U.S. government also repeatedly dismissed concerns of surreptitious scanning of these electronic passports, while still in the traveler's pockets. The U.S. government's public position is that the scanners are bulky and only will work at very short distances (about 4 inches). This position willfully ignores the fact that technology is constantly improving. If reading can be done at 4 inches today, it will be 4 feet in a year or two, and 40 feet a few years after that (see my column at DocFinder: 6729). There are many parts of the world where I would not want to travel with a passport in my pocket that could tell any properly equipped terrorist within easy striking distance that I'm an American.

Overall the picture is chilling. What is most chilling is the idea that the U.S. government has been actively trying to keep the passports from being secure. In effect, the government has been actively, and with full warning from many sources, trying to ensure that Americans will be at risk when traveling any place where someone might harbor bad feelings toward the U.S. What kind of decision process could possibly have concluded that putting one's own countrymen at risk was worse than having secure passports? The only thing I can think of is that the U.S. government must want to surreptitiously track passport holders from other countries, and the desire to do that outweighed the safety of Americans. Maybe there is another explanation, one that just involves mulish stupidity or obstinate shortsightedness about the pace of technical evolution. But, as a traveler, I am being put at risk. That's not something that I much like, whatever the explanation.

Disclaimer: Mulish stupidity is not a common Harvard trait, so the above observation is mine — not the university's.

Bradner is a consultant with Harvard University's University Information Systems. He can be reached at sob@sobco.com.

IBM software targets compliance

■ BY ANN BEDNARZ

IBM recently announced software aimed at helping companies comply with Basel II, the international banking accord.

The company's Risk and Compliance Basel II Information Management Offering combines data management and analysis tools to help handle the information banking institutions must collect and report in accordance with Basel II. Published by the Bank of International Settlements, Basel II is a standard for measuring risk.

IBM's Basel II platform — which the vendor says 35 banks now use — includes its DB2 Data Warehouse, WebSphere Information Integrator and Alphablox analytic software.

The bundle also is integrated with Fair Isaac's Triad adaptive control system, which includes specialized tools for risk analysis. Used together, the platforms can help banking institutions decide on customer and account management, scoring, collections, credit line management and marketing communications, IBM says.

Among U.S. retail banks, compliance and risk management is a key technology driver, according to research from Datamonitor. In the firm's survey of 100 IT executives at U.S. banks, 80% said enabling compliance with changing regulatory requirements is the most important driver of core systems investment in 2005.

Respondents plan to spend $2.6 billion this year, or 4.2% of their total IT budgets, on systems for achieving compliance with regulations such as Basel II, the Sarbanes-Oxley Act and the Patriot Act, Datamonitor says. That's up from almost 4% in 2004.

Enterprise price averages $500,000, not including the Fair Isaac TriadD software. ■

PSS Systems
continued from page 29

Sarbanes-Oxley Act, as well as an increase in litigation-related document discovery obligations. Enterprise content management vendors, such as EMC, FileNet, IBM and Open Text, offer products with version control, records management, collaboration and workflow features.

PSS Systems' software complements those companies' suites, Paknad says. "There's a whole diversity of information systems that keep certain kinds of business information, and generally those are unique to a business unit and department," she says. For example, a company might keep financial information in an SAP system and legal contracts in a separate content management system. "Atlas IPM acts as an overlay across all of the disparate systems and stores where companies keep data."

Atlas IPM consists of two main components: server-based policy management software and desktop-based enforcement agents. Policy Atlas is the suite's repository of corporate policies and schedules. Companies can oversee and authorize policies centrally, while delegating management responsibilities to staff in different locations and business units. If a legal matter requires turning over documents, companies can use Policy Atlas to handle corporate-wide notification and collection processes.

E-mail archiving on the rise

Among 300 companies surveyed by Gartner

have an e-mail archiving system in place, while 21% plan to implement one within 12 months.

Policy Point is the enforcement component that applies policies to information repositories. Agents deployed on user desktops and file servers tag unstructured content as it's created or received. The agents can move content if necessary — if a user creates a business contract that is supposed to be stored in a particular system according to corporate retention policies, the agent will move the document to that location. Policy Point agents also can override disposal schedules if a legal matter requires certain documents be saved.

Because Atlas IPM creates a policy and classification layer over current infrastructure, it's not disruptive to end users, Paknad says. "It's not a brand new repository, where users should put all information. It's a repository of policies and a pretty quiet, pretty invisible technology that leverages the repositories companies already have."

Enterprise pricing for the Policy Atlas and Policy Point software modules starts at about $100,000 each. ■

SpikeSource
continued from page 29

tual property as open source is combined with current legacy applications, analysts say.

A Forrester Research survey of 140 North American firms last year found that 46% of respondents use open source software and 14% have plans to bring open source into their data centers. But 39% of the respondents said they had no plans for open source software and said that lack of skills and support were the primary inhibitors.

As part of SpikeSource's effort to make the integration of open source into enterprise data centers easier, the company also announced that it was partnering with other open source companies — such as Black Duck Software, which provides tools to ensure that open source software meets licensing requirements, Red Hat, JBoss and Novell — to expand the open source products and services it can offer.

SpikeSource's competitors include SourceLabs, Gluecode, GroundWork and OpenLogic.

"They're all trying to resolve one of the side effects of the vibrant open source community, which is lots and lots of projects that are quasi-independent. They are trying to provide a single source so that you don't have to use different installation tools and have different scripts to deal with [when deploying these components]," says Michael Goulde, a senior analyst at Forrester.

"That will lead to a much higher probability of success. It's worked that the individual projects can't do it — it's not part of their scope. And the major vendors — such as IBM — haven't stepped up to the table yet." ■

Middleware is Everywhere. | Can you see it?

5

2

4

3

1

IBM

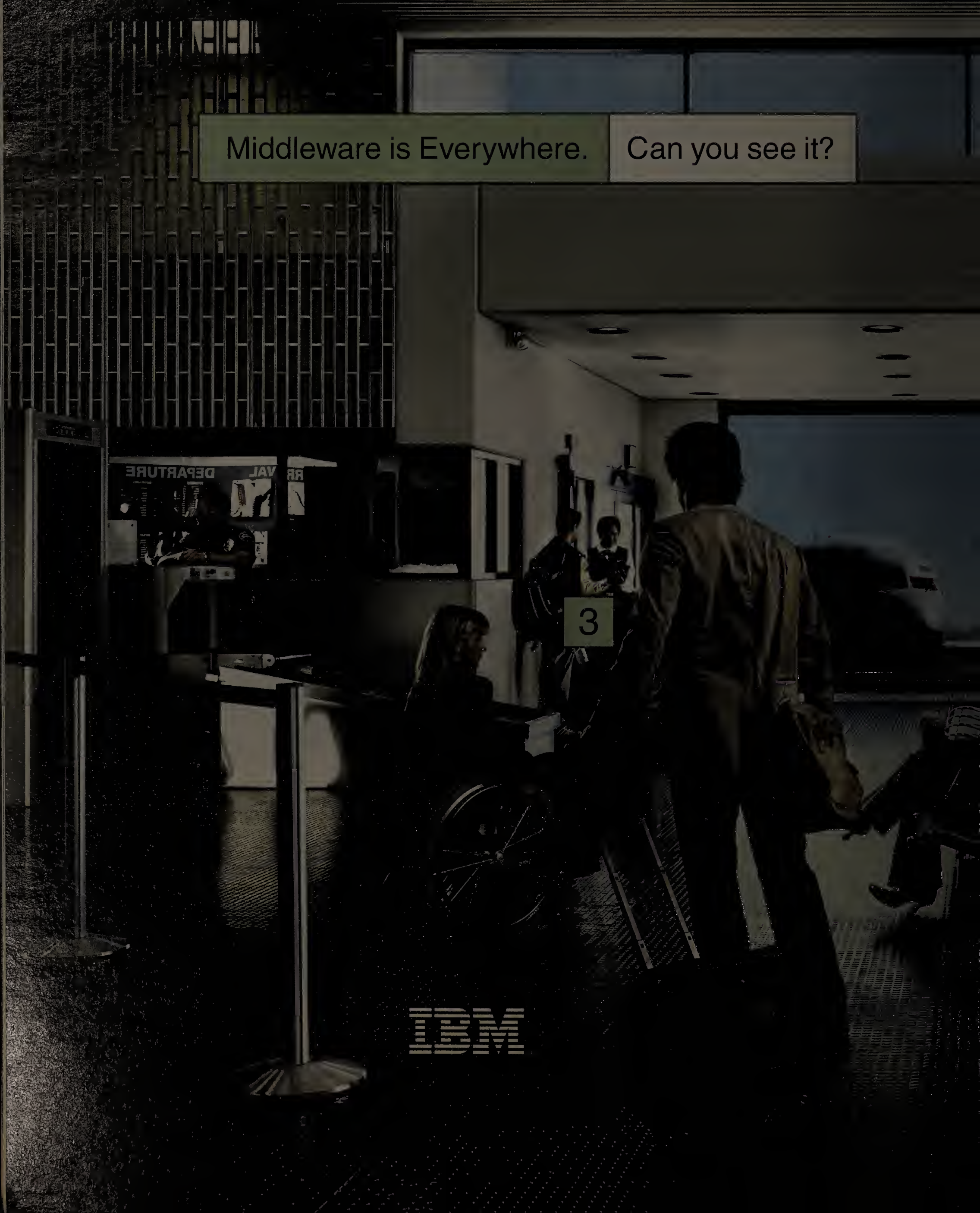
Middleware | Key

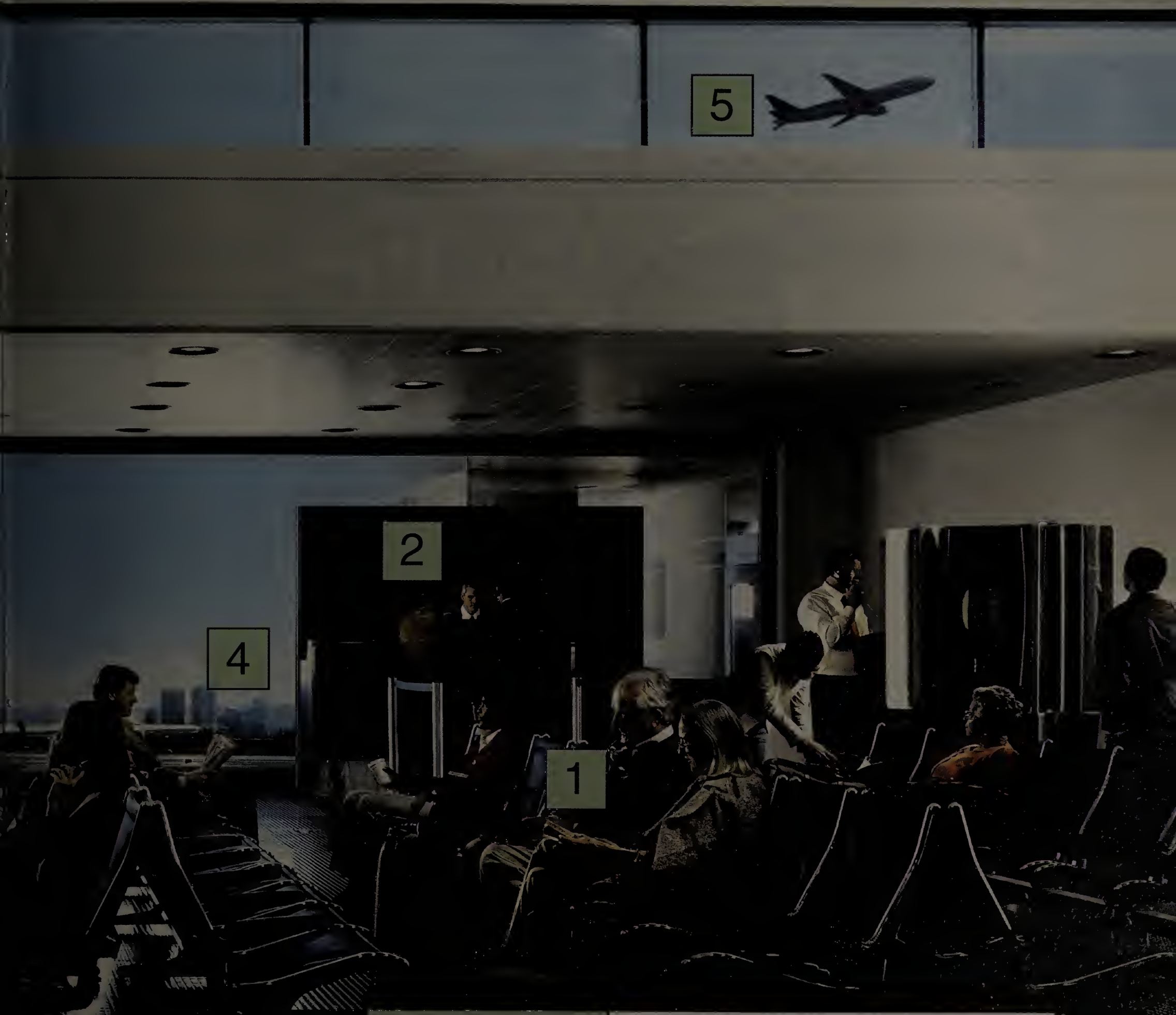
1. **Statistics from Asia retrieved quickly.**
2. **Paris client's portfolio accessed securely.**
3. **Critical information archived automatically.**
4. **Data kept within compliance guidelines.**
5. **Optimized storage supports heavy volume.**

MIDDLEWARE IS IBM SOFTWARE. The IBM TotalStorage® Open Software Family. It automatically helps manage and optimize highly complex storage environments. By centralizing information. By fully utilizing resources. By simplifying data compliance. Help slash long-term storage costs. On demand. Comprehensive, reliable storage management solutions from IBM.

Middleware for the on demand world. Learn more at **ibm.com**/middleware/resource ON DEMAND BUSINESS™

IBM, the IBM logo, the On Demand logo, and TotalStorage are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. © 2005 IBM Corporation. All rights reserved.


Middleware is Everywhere.
Can you see it?
3
IBM



DB2.

Key

1. Takes virtual tour of vacation spot.
2. Books flight with partner airline.
3. Dispatches service automatically.
4. Analyzes schedule data dynamically.
5. Business results reach new heights.

MIDDLEWARE IS IBM SOFTWARE. The powerful DB2 Information Management Software Family. With industry leading DB2 and Informix® databases, it's the most complete information management solution available. Built on open standards, it lets you access content from various sources. Integrate information, boost productivity, stay compliant. Plus gain insight to make better business decisions. On demand.

Middleware for the on demand world. Learn more at **ibm.com**/information ON DEMAND BUSINESS™

IBM the IBM logo, DB2, Informix and the On Demand logo are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. ©2005 IBM Corporation. All rights reserved.

SDLT 600 TASTE TEST

TEST #369

SDLT 600 Results :

Taste :	☐	**Speed :**	☑	**Manageability :**	☑
High Capacity :	☑	**WORM :**	☑	**Compatability :**	☑

COMMENTS

TESTED BETTER

In a blind taste test, the SDLT 600 was found to be less than appetizing. Test subjects' comments included, "if there is a hell, this is the food." Scientists have agreed to conduct the next round with condiments. As for data backup abilities, it passed with ease. The SDLT 600 has more capacity and more speed than LTO-2 and AIT-3. It also includes DLTSage™ diagnostic management software and DLT*ice*™ archival WORM functionality. How do we know? It's been tested. For more info and to see the whitepaper, visit DLTtape.com.

DLT

egistered trademark and the DLT trade of Quantum

ServiceProviders

■ THE INTERNET ■ INTEREXCHANGES AND LOCAL CARRIERS
■ REGULATORY AFFAIRS ■ CARRIER INFRASTRUCTURE

Short Takes

■ **AT&T** last week inked a three-year, $21 million contract with The ServiceMaster Co. ServiceMaster is essentially renewing its contract with AT&T, which provides a national IP VPN service to the company. ServiceMaster is a residential and commercial company that provides a host of services, including cleaning, lawn care, landscape maintenance, pest control and plumbing services. ServiceMaster uses the IP VPN service to communicate with its 5,400 company-owned and franchised service centers and offices. The company also uses the network to securely communicate with partners and suppliers.

■ **Occam Networks,** a supplier of Ethernet- and IP-based loop carrier equipment, recently announced an alliance with **Tellabs.** Tellabs will sell Occam equipment to North American carriers. Tellabs also has licensed Occam's Ethernet transport technologies for integration into its FiberDirect portfolio. Occam's broadband loop carrier products are designed to enable telecom providers to create broadband access networks capable of delivering services such as VoIP, IPTV and high-speed data over copper using IP and Ethernet protocols.

■ Managed Ethernet service provider **Yipes Enterprise Services** last week said it received a Series C round of funding of $24 million. The round was led by Crosslink Capital, along with Yipes' investors Norwest Venture Partners, JPMorgan Partners and Sprout Group, a venture capital affiliate of Credit Suisse First Boston. Yipes said the new round of funding exceeds the company's financial requirements to reach positive cash flow in 2006. In total, Yipes has raised nearly $94 million since July 2002, when it emerged from bankruptcy. Previously, Yipes was a poster child for the telecom meltdown, burning through about $300 million in funding between its founding in 1999 and its Chapter 11 bankruptcy filing in March 2002.

911 isn't a negotiable service

EYE ON THE CARRIERS
Johna Till Johnson

Is 911 service an optional feature, or an integral part of telephone service? After a 17-year-old girl couldn't get through to police when home intruders shot her parents, the state of Texas sued VoIP provider Vonage for "deceptive trade practices" for failing to offer built-in 911 services. Other states are following: Last week the governor of Illinois called publicly for VoIP providers to be forced to include built-in traditional 911, and New York is said to be planning a similar statement.

Vonage disagrees, arguing essentially that 911 is an option, not a requirement. Vonage customers don't receive built-in 911 service — they have to pay extra. Even when they do, Vonage's 911 service lacks critical emergency features such as location detection. Finally, Vonage says that while it would like to add comprehensive 911 features to its VoIP service, the incumbent local exchange carriers (ILEC) won't offer the necessary network access.

The ILECs' rebuttal: The real issue is cost. Vonage doesn't want to pay for integrating into the 911 infrastructure, they say. "There are existing procedures to connect to the 911 network today, which several [VoIP] providers utilize. Vonage has opted not to," says a BellSouth spokesperson.

There's a bigger issue at stake. Many VoIP advocates make the broader argument that 21st century technologies such as VoIP shouldn't be held back by expensive 20th century regulations such as those applied to 911, which they say stifle innovation and shortchange consumers.

In a world with global positioning services and instantaneous satellite connectivity, these folks say it's time to rethink how and where we connect to emergency services. Maybe emergency connectivity shouldn't even be a part of telephone service at all, particularly when better alternatives exist, they say.

That sounds reasonable. But is it? For one thing, these "alternatives" don't, in fact, exist — and it's not at all clear they'd actually be better. Assume every man, woman and child in the U.S. were issued a pocket device that connects to the global satellite network, pinpoints the user's location and provides one-button emergency access.

The service would be massively expensive to roll out and maintain. And its ability to deliver always-on services would be questionable. Batteries need to be replaced. Satellite doesn't work in hard-to-reach places, such as basements. Emergency devices can be lost (ever misplace a wallet or key ring?).

And last but not least, what organization should own and operate this brave new emergency infrastructure? (Do you really want the government getting real-time information on the whereabouts and movements of every citizen?)

More to the point, there's something fundamental about the linkage of emergency services and telephony. As Thomas Norling puts it in his brilliantly concise history of 911: "At the beginning of most all telephone operations was a need to provide emergency communications." (See www.nwfusion.com, DocFinder: 6730 for the rest.)

Norling is right. Vonage is wrong. 911 isn't optional, it's an integral part of telephony. VoIP providers should pony up the cash to integrate properly into the current 911 infrastructure, and if that increases costs and slows adoption, so be it.

Johnson is president and chief research officer at Nemertes Research, an independent technology research firm. She can be reached at johna@nemertes.com.

BT Infonet bolsters IP VPN services

■ BY CAROLYN DUFFY MARSAN

Global ISP BT Infonet is expanding its suite of IP VPN services by adding application-based configuration and monitoring tools.

BT Infonet's new Application Centric VPN is available with its IP VPN Secure, a private IP-based service built using Multi-protocol Label Switching (MPLS) technology. The service is available in 57 countries.

The managed service includes devices for optimizing application performance over a network, as well as software that provides increased visibility and detailed controls for users. It is designed to dynamically allocate VPN resources to meet the needs of business applications.

"The focus here is on managing application performance," says Jean-Noel Moneton, vice president of VPN Services for BT Infonet. "By giving the customer some level of visibility and some level of control, we end up giving him better network economics."

BT Infonet's new service automatically recognizes more than 160 applications from leading vendors such as SAP, Oracle and Citrix. Users can discover what applications are running on their networks and then set priorities in terms of the class of service each application will receive.

The service uses a network appliance from Ipanema Technologies (which has BT Infonet as a minority shareholder) to optimize application performance in real time. It also uses EMC Smarts software to automate network systems management and MetaSolv Software's operation support system software.

The service provides real-time outage and performance alarms should the Application Centric VPN fail to meet its application performance targets. Users receive regular reports to see how various applications are performing, as well as reports in response to particular problems. Other features of the Application Centric VPN service include support for compression, multicast and multiVPN.

BT Infonet's service is targeted at multinationals with at least 10 sites globally.

Pricing for the Application Centric VPN depends on the number and type of sites taking advantage of the service. For a network with 20 sites — 11 in Europe, five in the U.S., two in Asia and one each in South America and Canada — the service would cost approximately $35,000 per month, BT Infonet says. This price includes the port and the IP Applications Engine at each site, all the monitoring and application controlling software, and the full suite of applications reporting. These prices are for T-1-comparable access, although they do not include a router or local access line. ■

Legislation would prevent federal 'Net access tax

■ BY GRANT GROSS

A U.S. senator is pushing legislation that would prevent Congress from extending a long-standing telecom tax to Internet access.

Sen. George Allen (R-Va.) says legislation is needed after Congress' Joint Committee on Taxation in January suggested the possibility of an expansion of a 3% federal excise tax on telecom to Internet traffic, including e-mail and data services.

The federal excise tax, first enacted in 1898 to fund the Spanish-American War, raises about $6 billion per year. At points during the last 107 years, the tax has been eliminated, reinstated and raised to 25%. Congress made the tax permanent in 1990.

"We won the Spanish-American War over 100 years ago," Allen said at a press conference last week. "This tax represents an unnecessary service tax on consumers."

The Joint Committee on Taxation in January presented three options for the tax, one being to tax all Internet traffic. A second would extend the tax just to voice traffic over the Internet, with a third option redefining how long-distance calls are taxed, with no taxes on Internet data or voice.

In November, Congress passed the Internet Tax Nondiscrimination Act, which extended a moratorium on new Internet-only taxes passed by state and local governments. But that bill, also sponsored by Allen, didn't apply to the current excise tax. Allen's new bill wouldn't prohibit taxes on VoIP; that would be addressed under a separate bill likely to be introduced later.

The January report from the Joint Committee on Taxation noted that the growth of wireless-voice services and the Internet have created confusion about how the federal tax should be applied. "The present communications excise tax provisions were enacted before the development of most modern technology," the report said. "The proliferation of wireless communications technology and the Internet, and in particular broadband access, has blurred the lines between 'data' and 'voice' and between the functions of transmission and application. Consequently, service providers have found it increasingly difficult to determine which services are taxable communications services and which are nontaxable information services."

Asked why a bill was necessary to prevent a tax on Internet access that does not yet exist, Allen said it was important to head the idea off before it gains momentum. In addition to the Joint Committee on Taxation proposal, the Internal Revenue Service last July asked for public comments about whether VoIP should be subject to telephone taxes.

Representatives of the Progressive Policy Institute, a liberal think tank, and Americans for Tax Reform, a conservative policy group, both endorsed Allen's efforts.

Robert Atkinson, vice president of the Progressive Policy Institute, said he disagreed with the elimination of the federal excise tax during the U.S. government's current budget deficit. But an additional tax on Internet access could slow the U.S. economy and discourage IT investors, he said.

"We're a long way from maturity in the industry," he said. "One of the things that's made the Internet attractive [to investors] is the light tax burden."

Gross is a correspondent with the IDG News Service.

IPSWITCH™ Collaboration Suite

Ipswitch Collaboration Suite, the solution for small and mid-sized business collaboration that just works. Use Microsoft®Outlook® or your browser to connect to a powerful industry-leading messaging server. Communicate in real time with anyone in your company using secure instant messaging. Streamline group collaboration with shared calendars and free-busy meeting scheduling. Reduce junk e-mail and stop viruses. All this, and Ipswitch Collaboration Suite is easy to install, manage and use. Play it "safe" like Frank. Or be smart. Go to www.ipswitch.com and find success with Ipswitch Collaboration Suite.

- Smart
- Proven
- Reliable
- 60 million mailboxes worldwide

IPSWITCH

www.ipswitch.com or call 800-793-4825

©2005 Ipswitch, Inc. All product names are the property of their respective owners.

RECLAIM YOUR EMAIL

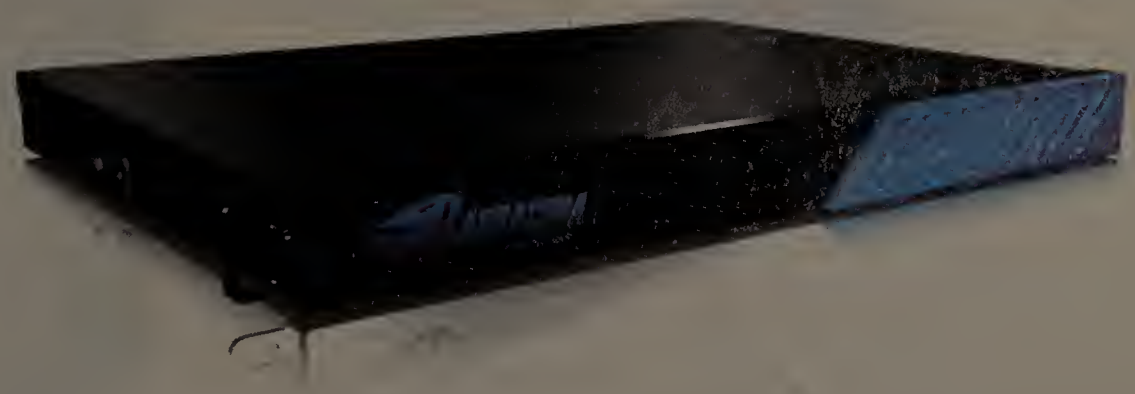
Visit us at Info NECC
Booth #358
June 27-30 Pittsburgh, PA

Spam and virus protection at an affordable price.

- No per user license fees
- Prices starting at $1399
- Powerful, enterprise-class solution

Barracuda Spam Firewall

BARRACUDA NETWORKS



Order a free evaluation unit at
www.barracudanetworks.com

POWERFUL EASY TO USE AFFORDABLE

Aggressive Reseller Program
Get more info by visiting www.barracudanetworks.com/NECC
or by calling 1-888-ANTI-SPAM or 408-342-5400

LINKSYS®
A Division of Cisco Systems, Inc.

Speed and Range eXpansion

Faster and Farther Than Ever Before!

Wireless-G with SRX

WRT54GX
Wireless-G
Broadband Router
with SRX

Speed and Range eXpansion

Watch streaming video or play multi-player games faster than ever before. And do it comfortably from places that were previously unreachable. Introducing the Wireless-G with SRX series, the newest, fastest, most powerful addition to the Linksys Wireless-G family.

Enjoy the Wireless-G with SRX experience:

- Up to 8 times faster than standard Wireless-G
- Increased wireless range up to 3 times farther
- Reduced dead spots in coverage area
- Compatible with Wireless-G and B networks

WPC54GX
Wireless-G
Notebook Adapter
with SRX

Visit www.Linksys.com/SRX today for product details, or call our Advice Line at
1-800-737-7201

LINKSYS® Partner Connection

CDW

STAPLES

Office DEPOT

that was easy.

Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2005 Cisco Systems, Inc. All rights reserved.

CISCO SYSTEMS

Net.Worker

■ PRODUCTS, SERVICES AND STRATEGIES FOR TYING TELEWORKERS TO THE ENTERPRISE

Cisco aids govt. in business continuity

■ BY TONI KISTNER

To help public agencies comply with the federal government's Continuity of Operations mandate, Cisco recently announced its VirtualCOOP Solution and MeetingPlace Crisis Management Application at the Federal Systems Expo in Washington, D.C.

COOP requires all federal agencies to develop a plan for continuing operations during and following a disaster, and the ability of employees to telework is crucial. Last June, President Bush issued a directive outlining COOP objectives. Steps include identifying alternative operating facilities, providing interoperable communications, and validating the capability through tests.

Cisco breaks down its VirtualCOOP Solution into four parts:

- Network (component, device, solution and system-level redundancy).
- Application (data center solutions, content-delivery services, storage networking and data replication).
- Communications (distributed, central office-based gateways and distributed call centers with integrated messaging).
- Workforce (wireless integration, office-in-a-box products and telework).

"This is like mesh COOP," says Christopher Baum, an analyst at Gartner. "If you start distributing the network, you get huge disk repositories supporting individual people at remote locations. You need a system for bringing them together in a method that's recoverable and actively self-managing. So when you lose a node on the mesh you don't lose the entire mesh. There hasn't been the technology before to do this."

Cisco's VirtualCOOP Solution relies on current (and emerging) Cisco technologies, such as VPN tunnels connected to high-availability networks. The MeetingPlace Crisis Management Application is new, and was developed by Cisco and Apptis. The product lets federal agencies and state and local police and fire squads establish a permanent conference bridge for VoIP communications. When a user calls in and types in an ID code to establish the bridge, network resources are dynamically allocated to the connection.

Cisco leaves the people aspects of agency resilience and COOP — succession planning and teleworker training — to partners Accenture, IBM, HP and Northrop Grummand. Partner SAIC is conducting a trial (setting up Cisco VPN connections and VoIP phones) with a civilian government agency, says Chris Shenenfiel, Cisco's federal industry solutions manager.

"Government IT execs are beginning to discover networking can get around many of their problems," Shenenfiel says. "A snowstorm in D.C., shouldn't disrupt operations in Dallas. It was like a revelation to them."

Cisco is targeting civilian government agencies, including the Census Bureau, Small Business Administration and the Smithsonian Institute. The telework compliance numbers are low: Shenenfiel says they're wrestling with some problems.

"The Department of Defense has its own programs, but civilian agencies aren't so far along," Shenenfiel says. "Funding right now is keenly focused on Homeland Security, and other agencies that aren't directly aligned with [national] defense still need to achieve these mandates. But where's the money? Now they have a penalty for not teleworking but no funding for telework."

So agencies must think creatively. Now federal employees are compensated $100 per week for commuting; money that could be used to fund telework, Shenenfiel says. They're also beginning to grasp that using telework to achieve COOP can pay for itself by cutting real estate costs.

When agencies have money to fund IT projects, Cisco is helping them — with COOP in mind. When rebuilding a data center, for instance, agencies can distribute servers to locations across a self-configuring, self-healing network, and establish primary and back-up centers in other places.

"One thing we've learned is to back up your laptop, but nobody does," Baum says. "But when users' file replication and back-up happens in the background, they won't need to keep paper copies and back-up files that can get lost and pose a security risk. Then you'll have a variably connected and secure environment that knows when the client's connected to a 115K bit/sec GPRS link or an unsecure Wi-Fi network. That's the level of management that's been missing." ■

Fanning out

Three drivers pushing distributed work in the federal government.

- **Presidential COOP directive:** Federal Preparedness Circular 65 provides guidance to federal executive branch agencies on developing "viable and executable" contingency plans for the Continuity of Operations. When normal operations are disrupted, COOP ensures critical functions will be performed.
- **Federal telework mandate:** Public Law 106-346, Section 359 (passed Oct. 23, 2000) requires each executive agency to establish a telework policy under which all eligible employees can participate to the "maximum extent possible" without "diminished performance."
- **Penalties for non-compliance:** Agencies under the Commerce, Justice and State appropriations bill that don't offer telework to eligible workers will lose $5 million under a provision passed as part of the fiscal 2005 Omnibus spending bill.

Short Takes

■ **Zyxel** has announced the **Zywall P1 Personal Internet Security Appliance,** a portable VPN and firewall for mobile users. The 3-by-5-inch device includes Ethernet WAN and LAN ports and a USB port. Security includes a stateful packet inspection firewall, IPSec VPN client and end-point management, and costs $299.

■ **Tritton Technologies** has introduced a line of network-attached storage devices for small offices and consumers. Products come in 160G, 200G and 250G-byte models, and include an FTP server for sharing files over the Web. Prices range from $199 to $299; an enclosure-only model costs $99.

Group tries to spur telework

■ BY GRANT GROSS

A group of technology vendors and U.S. government technology leaders recently launched an effort to encourage federal employees to telework. The Telework Exchange, announced at the FOSE government IT show in Washington, D.C., comes on the heels of a survey published in January that showed nearly two-thirds of U.S. government workers haven't been allowed to telework even though the U.S. Congress has established penalties for agencies that don't have telework options.

CDW Government (CDW-G), which released the survey, founded the Telework Exchange with Intel, Citrix and Juniper Networks. Since the survey was published, CDW-G has found only a 1% increase in the number of federal workers teleworking. Telecommuting is especially attractive in the Washington, D.C., area as a way to avoid traffic and reduce pollution. Increased teleworking also can help government agencies attract workers and operate in times of security threats, says Karen Evans, administrator of the Office of the Electronic Government and Information Technology at the White House Office of Management and Budget (OMB). "We want to eliminate the telework gridlock," she adds.

The Telework Exchange will include an advisory board with congressional, OMB and industry representatives. "The objective is to ... move teleworking into the fast lane," says Stephen O'Keeffe, executive director.

Gross is a correspondent with the IDG News Service.

Dirty work

A U.S. government commuter driving a round trip of 40 miles a day in an SUV would spend about

$8,100

a year commuting, and pump 6.8 tons of pollutants into the air.

SOURCE: TELEWORK EXCHANGE

Slow Systems?

BREAKTHROUGH TECHNOLOGY KEEPS THEM RUNNING AT TOP SPEED

One of the most common questions that comes up when talking about Diskeeper® is "Why pay for a defragmenter when Windows has one for free?"

To answer this question, let's compare defragmentation to housecleaning. Everyone's house gets dirty, and there are basically three ways to handle it:

1. Do nothing. The house gets dirtier and dirtier, stuff starts to pile up, the smell gets worse and neighbors start calling the health department. Eventually the house gets so dirty that it's uninhabitable, so you move out and find another place to live. (This scenario is similar to never defragmenting.)

2. Clean it yourself. This usually requires carving at least an hour or so per day out of your free time. (This scenario is like defragmenting your systems with a manual defragmenter.)

3. Hire a housecleaning service to come in and clean on a regular basis. (Automatic defragmentation.)

Do it yourself?

#2 seems like a reasonable solution. After all, plenty of people clean their own houses, right? In theory, yes. In reality, things come up—weekend plans, long work hours, etc. You might only have a few minutes to straighten up, or you might skip a couple of day's worth of cleaning altogether. End result: the house is rarely as clean as it could be, and when you do clean, it takes much longer than it should. Likewise, the process of manual defragmentation takes so long and involves so much IT staff time that it rarely gets done.

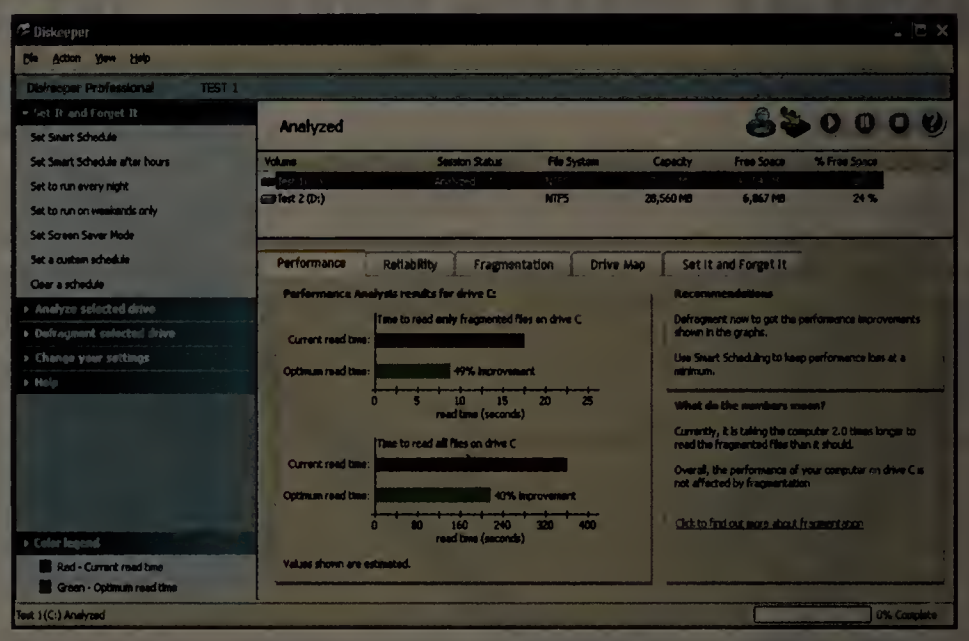
The most effective way to keep your house clean is to have it done automatically, on a regular basis. And the most effective way to keep your systems running at top speed with maximum reliability is to have them defragmented automatically.

Find the right solution

Let's say you hire a cleaning service to come to your house once a week and scrub the daylights out of it. They vacuum carpets, clean windows, polish furniture, organize the attic, etc., etc. It takes them all day and well into the evening. And while you like having a clean house, it's annoying to have to wait to eat dinner because someone is polishing the chrome on your oven door. Or to have to park on the street because someone was midway through straightening up the garage just as you got home from work. The same is true of defragmentation. A defragmentation run that kicks off at the wrong time can turn into a major headache and seriously disrupt your organization's workflow.

Automation with convenience

The perfect cleaning service is one that works around you. You can tell them when you want them to clean, or they can decide how often to clean based on how quickly your house gets dirty. They take care of the big stuff first—counters, floors, bathroom—so that you have a clean house as quickly as possible. Minor chores, like polishing the chrome in the kitchen or cleaning the garage, are done at times when they won't inconvenience you. And if they do happen to be cleaning a room you need to use, they get out of your way immediately.



*Keep your systems running fast — **automatically.***

That's how Diskeeper 9, The Number One Automatic Defragmenter™, works.

Diskeeper 9:

The Number One Automatic Defragmenter

Diskeeper is a software system that completely eliminates the problems caused by fragmentation. Diskeeper 9 uses unique adaptive technology that works around your organization's workflow. You can implement Diskeeper 9 on every server and workstation right from your own desktop. Once Diskeeper is deployed, the problem of fragmentation simply goes away. Operation of Diskeeper 9 is almost completely transparent, which is why we call it the "Set It and Forget It"® defragmenter!

See the difference for yourself. Download the FREE 30-day trial edition of Diskeeper 9 now!

TRY DISKEEPER FREE FOR 30 DAYS

www.diskeeper.com/nww9

For volume license pricing and government or educational discounts, call 800-829-6468 phone code 4318

Diskeeper 9

The Number One Automatic Defragmenter

Sponsored by:

Executive Software®

©2005 Executive Software International. All Rights Reserved. Diskeeper, The Number One Automatic Defragmenter, Set It and Forget It, Executive Software and the Executive Software logo are registered trademarks or trademarks of Executive Software International, Inc. in the United States and/or other countries. Microsoft and Windows are either registered trademarks or trademarks owned by Microsoft Corporation in the United States and/or other countries. **Executive Software International, Inc.** • 7590 N. Glenoaks Blvd. Burbank, CA 91504 • 800-829-6468 • **www.executive.com**

Technology Update

■ AN INSIDE LOOK AT TECHNOLOGIES AND STANDARDS

Category 7 cabling boosts throughput

■ BY MARILYN MICHELSON

As Gigabit and 10G Ethernet networks take hold in companies that need more speed, the copper physical layer of cabling has evolved to easily handle future applications. One of the most recent improvements to infrastructure is Category 7 cabling (sometimes called Class F).

The Cat 7 standard for high-bandwidth cabling was developed in Europe and is gaining increasing recognition in the U.S. It is formally referred to as international standard ISO/IEC 11801-2002.

Cat 7 cabling technology accommodates up to 600 MHz of bandwidth, the most for any type of copper cabling. Previous cabling technologies were based on conservative performance standards, such as Category 5e — 100 MHz, and Category 6 — 250 MHz. Early adopters of new technology such as 10G Ethernet, or companies concerned with electromagnetic interference to an environment such as a factory floor, tend to use Cat 7 cabling.

Cat 7 cabling is fully shielded — each pair is shielded with a foil screen, and the cable itself has an overall shield. Some versions also add in a braid screen between the cable sheath and the shielded pairs. The cabling also is immune to alien crosstalk — that is, noise from adjacent cables outside its own sheath.

Until now, Cat 5e and Cat 6 cables have used cancellation techniques to handle the effects of noise from within the cable sheath. The biggest problem to copper cable with 10G Ethernet transmission is noise from outside the sheath.

Price/performance

Cat 7 cabling is the biggest pipeline for balanced cabling. But it costs roughly three times as much as Cat 6 plenum cabling, which is priced at $380 for a 1,000-foot reel. Companies that have a planning horizon of 10 years might be able to justify the cost of a Cat 7 installation (cable and connectors) because it should save money over alternative cabling methods that can handle applications that require much more bandwidth.

One way to look at this Cat 7 cable is to think of it like the old "Type 1" cable, but with four pairs. This cable offers the user a choice based on the style of connector installed with it (RJ-style and non-RJ-style).

With the non-RJ-style connector, it offers application sharing. With the RJ-style, the infrastructure becomes backwards compatible and interoperable.

For this cabling technology to become more mainstream, an increasing number of equipment manufacturers need to design a Cat 7 interface on their hardware. Companies also will have to grow accustomed to a different interface. And the cabling has a larger diameter than Cat 6 because it's double shielded and typically uses a 23 American Wire Gauge bare copper conductor (vs. 24 AWG for Cat 6, 5e, 5 and others).

In addition to pricing this class of cable and connector, certification by a National Research Test Lab is important. This means the lab's mark will appear on the cable jacket. The mark shows that the equipment has been tested by a nationally approved test lab for safety and performance and that it complies with the international Cat 7 standard's performance specifications.

A Cat 7 product lends itself to new bandwidth, access, storage and speed demands. Depending on your needs and future goals, a cost-benefit analysis that compares this latest copper cable technology with its competition's performance can help determine what to use.

Michelson is president of Business Communication Services, which publishes BCS Standards Updates covering copper, fiber, coax, and wireless media. She can be reached at randm@volcano.net.

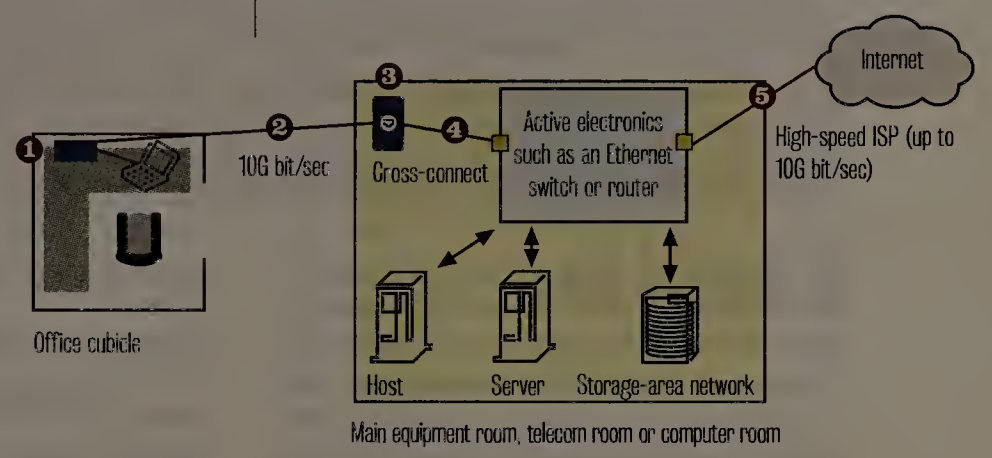
Got great ideas

■ *Network World* is looking for great ideas for future Tech Updates. If you want to contribute a primer on a specific technology, standard or protocol, contact Amy Schurr, senior managing editor, features (aschurr@nww.com).

■ HOW IT WORKS

Category 7 cabling

This cabling standard meets the need for speed by handling 10G Ethernet traffic.



1. An equipment cord extends approximately 3 feet from the PC or laptop and connects to a Cat 7 telecom outlet.
2. The Cat 7 cabling continues from the telecom outlet to the patch panel.
3. The Cat 7 cable terminates at the patch outlet.
4. Cabling continues with equipment cable that extends approximately 23 feet from the patch panel and connects to a Cat 7 connector on the active equipment.
5. Internet access speed depends on the contract negotiated with the ISP.

Ask Dr. Internet

By Steve Blass

Is there a system that can produce Web content from several materials and then produce a set of mostly static Web pages that we can deploy to a site hosted by our ISP?

Take a look at Apache Lenya (http://lenya.apache.org). Lenya is a content management system that uses Apache Cocoon to provide a system that can build Web sites for deployment to third-party hosting sites. Lenya has several life-cycle management features, including document creation, management and WYSIWYG HTML editing support. The executable versions are great for getting started. For production use, you will want to build your own from scratch. To build Lenya, download the Java source distributions of Cocoon and Lenya from apache.org, and unpack them both to the same parent directory. Build Cocoon first by running the "build" command in the Cocoon directory you just created. Then change to the Lenya source directory and follow instructions in the Install-SRC.txt file, and run the "build" command in the Lenya directory. After that, you can create and edit Web sites by pointing a browser at http://localhost:8888. You then can publish content to a folder and copy the new site to the ISP host.

Blass is a network architect at Change@Work in Houston. He can be reached at dr.internet@changeatwork.com.

Intelligent Infrastructure, Intelligent Business

Overlaying the Internet with an intelligent infrastructure unleashes the next generation of business potential

As amazing a business tool as the Internet has become, the fact remains that organizations have just scratched the surface of its far greater potential. The ability of Voice over IP (VoIP) to radically reduce fundamental communications costs is one early indication of the Internet's transformational capabilities. The unique insight into Internet security patterns and trends can allow a managed security services provider to give businesses the extra measure of security protection demanded today. Radio frequency identification (RFID) projects are literally redefining the way manufacturers and their partners interact. From these examples and others, it is clear the emergence of intelligent infrastructure services is bringing the potential of the Internet to full flower.

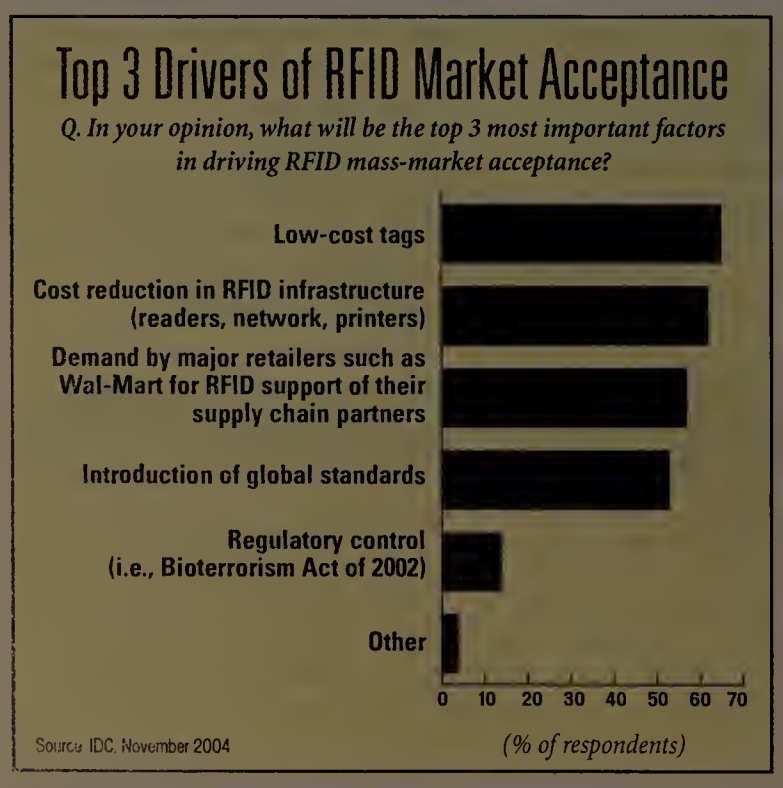
It would be more than three decades before the short-haul railroads that sprung up everywhere starting in the 1830s would finally be interconnected and transformed into a national rail system. This took such a long time simply because railroad operators had to use sluggish, unreliable overland mail services to coordinate this vast effort.

But once telegraph lines were installed right alongside the rail beds, two-way communication became almost instantaneous. Rail development soared as a vast national network took shape. And it all happened because the original system was overlaid with an *intelligent infrastructure: the telegraph network.*

Thus, a network faced with a critical level of usage and a growing complexity threatening its usefulness was instead transformed into a veritable engine of progress and growth. The rest, as they say, is history.

The same can be said today about the Internet. This network of networks holds almost limitless potential to link businesses to partners, suppliers, and customers in dynamic, interactive ways. The vision of a supercharged Internet will reach its full potential only if these links and connections can be made secure, reliable, and adaptable. In other words, like the early railroads of 175 years ago, the Internet needs an overlay of intelligent infrastructure. The Domain Name System (DNS) was the critical intelligent infrastructure that linked requests for user-friendly domain names to more complex IP addresses, which helped make the Internet accessible to the masses. Similarly, intelligent infrastructure will play a critical role in unlocking the tremendous business potential of the Internet as it grows.

Think of it this way: Intelligent infrastructure for the Internet will provide several, if not all, of the following key network enhancements—scalability, security, interoperability, availability, adaptability, and visibility—to literally change business processes and their economics. Already, intelligent infrastructure is enabling some of the most exciting business applications, such as VoIP, highly touted RFID-enabled supply chains, and mobile digital content delivery systems. And that's just for starters.



The drivers

Like the telegraph of a bygone era, intelligent infrastructure and intelligent infrastructure services are not technologies in search of a market or application. Quite to the contrary, the development of intelligent infrastructure services is intimately linked to today's major business and network drivers. These drivers include:

- **The growing use of the Internet for mission-critical applications.** During the year-end holiday shopping period last year, shoppers placed some $9 billion of orders online. That number should double in three years. But growth will be stopped dead in its tracks and even recede rapidly if consumer confidence in secure online transactions doesn't continue to grow in tandem.
- **The rapidly rising tide of regulatory compliance.** The business lexicon today is spiked with an alphabet soup of acronyms referring to new compliance regulations related to business data. From SOX to HIPPA to CALEA and so on, these regulations are placing heretofore unheard-of demands upon IT managers to maintain a scalable security framework to comply with internal and external audit requirements.
- **The fight against phishing and identity theft.** These two culprits, left unchecked, would be a big glass of icy cold water thrown in the face of Internet commerce, and the ramifications would be disastrous for so many kinds of organizations that have invested so heavily in e-commerce infrastructures.
- **The interoperability mandate.** Everyone knows that business-critical communication is trending outside the four walls of the organization or, in network terms, far beyond the firewall. The most important network and data links are among a business and its partners, customers, and suppliers. If the underlying network infrastructure doesn't have the intelligence to recognize and accommodate the disparate systems it inevitably encounters, growth of these vital communications links will surely be stunted.
- **The business continuity mandate.** Several years ago an industry pundit declared, "The network is the computer." The contemporary version of that truism is: "The network is the *business*." Just ask executives at an airline or hotel, or a modern manufacturing operation. If workers and

smart machines can't access and swap information, work for all practical purposes grinds to an ugly halt. Real costs accrue. Jobs and careers are jeopardized. The network has to be solid and stable, without compromise.

VeriSign answering the call to action

While the items above are noted as "drivers," IT managers usually refer to them as "formidable challenges," among other things. For IT managers, who have been working on very tight budgets over the last several years and are being pushed to support core business requirements and applications, the mere thought of meeting these challenges is daunting.

This is where VeriSign enters the fray. With its focus on providing and shaping the Internet's intelligent infrastructure, VeriSign is singularly dedicated to enabling businesses to find, connect, secure, and transact across today's complex Internet, telecommunications, and converged networks.

Perhaps most widely known for its Domain Name Registry Services, VeriSign in fact operates an intelligent infrastructure that processes an astonishing *14 billion* Web and email lookups each day. In North America, the greatest of all commercial marketplaces, VeriSign handles more than 37% of all e-commerce transactions, securely processing some $100 million in daily online sales.

By leveraging its rich and deeply experienced Internet legacy along with key technology acquisitions made in recent years, particularly in the digital content management area, VeriSign is positioned as the leader in providing intelligent infrastructure services at just the right time in business history.

Intelligent infrastructure in action

In many ways, intelligent infrastructure is synonymous with the most exciting aspects of network convergence and the blossoming of next-generation networks. VeriSign's expertise is already delivering results to IT professionals. In the red-hot area of Managed Security Services (MSS), VeriSign has leveraged its unique experience and insight into Internet security patterns and trends to provide unparalleled intelligent MSS. These services hit many IT security sweet spots, such as the growing problem of phishing or identity theft, as well as endpoint protection and managed vulnerability protection services.

"As enterprises face external forces that impact their business, such as hacker attacks, and cost, compliance, and complexity issues, they are looking to Managed Security Services Providers to help them with their network security. However, point solutions and MSSPs without unique differentiators do no good. With cyber attacks increasing in size and sophistication, they need unique insight into trends within their networks, across networks, and the Internet to make sure appropriate security protections are taken."

—Judy Lin, Executive Vice President and General Manager, VeriSign Security Services

When it comes to RFID-enabled supply chains, where electronic "tags" are poised to replace the current barcode system, VeriSign is making it possible for manufacturers and their partners to get more fine-grained, real-time inventory intelligence. Forrester Research maintains that new intercompany RFID projects will require advanced technologies to manage the sheer volume and complexity of RFID data. Forrester says partnerships between VeriSign and leading data synchronization vendors will help companies leverage and exploit RFID while at the same time preserving existing technology investments. Developments in RFID are providing scalable IP data sharing and trust services, enabling demand-driven supply chains, and increasing visibility.

VoIP carries the promise of sending a lot of today's communications costs through the floor. But for service providers to deliver on this promise to eager enterprise customers, they must first undertake a lot of basic blocking and tackling, such as providing secure connections to allow VoIP to pass through despite the large number of ports to be opened within a corporate firewall. VeriSign intelligent infrastructure services will provide all this and more to allow carriers to deliver the full benefits of VoIP while addressing their own needs to bridge Internet and telecommunications infrastructure.

VeriSign has also been active in the nascent digital content services area. A new VeriSign service offering allows mobile network operators to respond on a global scale to new service demands, from both businesses and consumers, for multimedia and interactive digital content delivered over mobile devices. These include intelligent messaging services to help businesses mobilize communication, collaboration, and workflow applications on just about any digital mobile device.

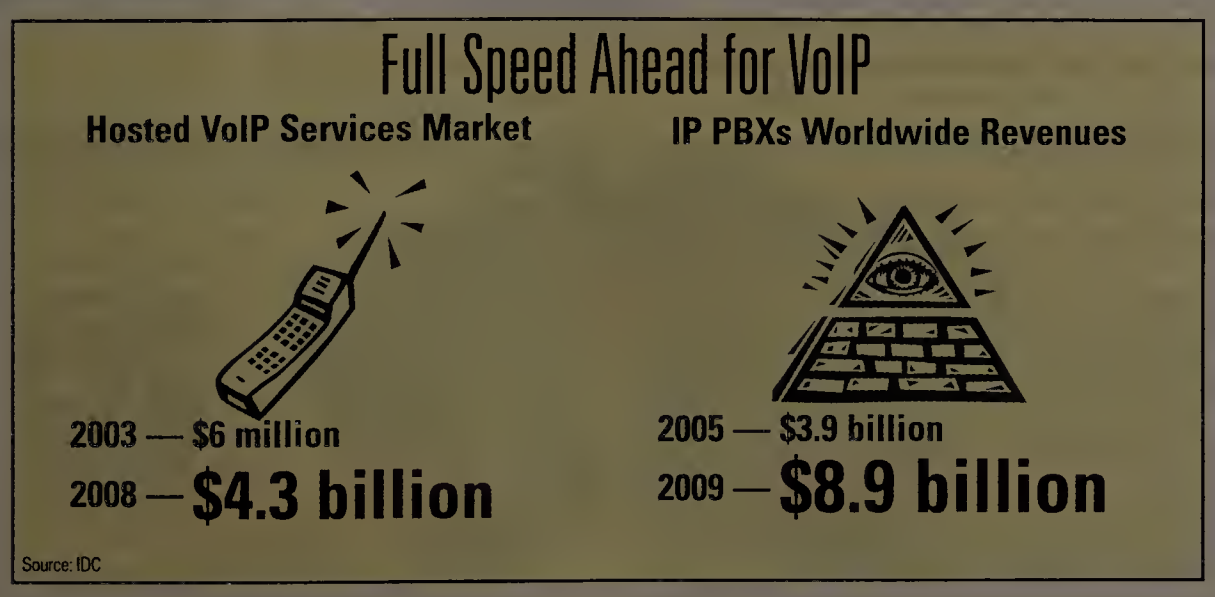
VeriSign®

A good example of intelligent infrastructure in operation is as follows: A sales executive is roaming on her cell phone (1), which switches over to an IP-based network (2), to make a transaction (3) in which content is secured (4) and delivered (5) back through that same connection. In this case, VeriSign has provided her with five different intelligent infrastructure services—transparent to her and the vital function she just fulfilled.

A matter of focus

This is just one example of how VeriSign has exploited its rich heritage of supplying Internet services to meet some of the most pressing challenges IT managers face as they struggle to meet today's hot IT issues of cost, complexity, and compliance. VeriSign is offering that overlay of intelligent infrastructure services essential to providing seamless, transparent interoperability among various network functions, clearing away obstacles to completing large IT projects that drive competitiveness.

Ultimately this vision and experience can pay significant dividends to enterprise IT managers who understand the potential of an Internet-based network overlaid by intelligent infrastructure services.



GEARHEAD INSIDE THE NETWORK MACHINE

Mark Gibbs

Open source opens opportunities

First off this week, do you have a recommendation for (or a warning about) a hosting service? We're looking for good management features (particularly for lots of e-mail accounts), good pricing (natch) and good support. Can such a thing be found?

Anyway, last week we mentioned the forthcoming release of Knoppix 3.8.1. Well, it's here. You can find a note about this version at Distrowatch (www.nwfusion.com, DocFinder: 6734), which also lists the FTP and BitTorrent download links.

As discussed, this release of Knoppix includes UnionFS, a stackable unification file system that merges the updated contents of multiple directories but keeps their original physical content separated.

The UnionFS Web site (DocFinder: 6735) describes the system as "useful for unified source tree management, merged contents of split CD-ROM, merged separate software package directories, data grids and more. UnionFS allows for any mix of read-only and read-write branches, as well as insertion and deletion of branches anywhere in the fan-out. To maintain Unix semantics, UnionFS handles elimination of duplicates, partial-error conditions and more."

The Knoppix implementation of UnionFS merges the Knoppix RAMdisk with the read-only file system on the boot CD so you can modify any read-only file as if it was writeable.

UnionFS is part of a project called the File System Translator, or FiST. The goal is to address the problem of file system development, a critical (as well as time consuming and expensive) area of operating-system engineering. The FiST site notes: "Even small changes to existing file systems require deep understanding of kernel internals, making the barrier to entry for new developers high. Moreover, porting file system code from one operating system to another is almost as difficult as the first port."

FiST, developed by Erez Zadok and Jason Nieh in the computer science department at Columbia University, "combines two methods to solve the above problems in a novel way: a set of stackable file system templates for each operating system, and a high-level language that can describe stackable file systems in a cross-platform portable fashion."

The idea is that with FiST, a stackable file system would need to be described only once. Then FiST's code-generation tool would compile one system description into loadable kernel modules for different operating systems (currently Solaris, Linux and FreeBSD are supported).

The project claims that with FiST, "code size and development time are reduced significantly, while imposing a small performance overhead of only 1% to 2%. These benefits are achieved, as well as portability, without changing existing operating systems or file system."

This is exciting stuff. And while we're talking about Knoppix, we also should mention another interesting Linux distribution (www.yeslinux.org), which was conceived of as "the premier distribution for a [small office/home office] that [wants] to create or has an existing Internet business." Yes Linux is intended to be secure and easy to use, and a completely integrated distribution.

Talking of usability, we just received Xandros Desktop, arguably the best attempt, so far, at a truly user-friendly Linux, achieving what one reviewer, Robert Storey, describes as "putting a point-and-click interface on the untamed beast — think of it as Debian with pizazz" (DocFinder: 6736).

Storey appears to have been very impressed with the product from the start of his review: "There is not a whole lot to say about the installation, except that Aunt Tilly could do it with her eyes closed (unless she's dead). Xandros boasts superb hardware detection, so unless you've accidentally mistaken a Macintosh for a PC, the install procedure should go smoothly."

Robert comments, "There is a running joke that you can install Xandros on a Windows user's hard drive, and he or she won't even notice. That, of course, is an exaggeration — surely our hypothetical Windows user would wonder what ever happened to Solitaire." This is encouraging, as the goal of a workable non-Windows desktop appears to be getting nearer.

These projects indicate there's an astounding amount of technology being developed. No matter how much effort is put into developing services and technologies for proprietary operating systems, over the next few years open source development will provide a bigger foundation for richer and more sophisticated operating-system platforms than anything any vendor in the commercial market can achieve.

Your thoughts on hosting, Knoppix, UnionFS, FiST, Xandros or anything else you please to gearhead@gibbs.com.

Cool Tools

Quick takes on high-tech toys

By Keith Shaw

Every once in a while you need to stop looking at the big picture and focus on the little things. Here's some little things that recently caught our attention:

Laptop Legs will help your computer stay cool and let you leave the notebook stand at home.

The scoop: Laptop Legs, about $20, from LapWorks (www.laptopdesk.net)

What it does: If you're looking to elevate your notebook PC to let it cool down or even improve typing ergonomics but don't want to buy an expensive separate laptop stand, then these plastic laptop legs might be just the solution. By placing two of them on the bottom of your notebook, you can elevate the back up by 1 or 1.5 inches to let hot air from the notebook escape or let cool air in.

Why it's cool: The legs have adhesive that stick to your notebook, so you don't have to bring a separate notebook stand when you're traveling. These also are probably the most inexpensive way to help dissipate heat from the notebook that we've seen (other than trying to create your own notebook stand).

Some caveats: If you use your notebook with a docking station, you might encounter some problems with the placement of the Laptop Legs. On our Compaq Evo notebook, we discovered that the back of it was exactly where the Laptop Legs were placed, preventing us from connecting to the docking station until we removed the legs.

Grade: ★★★½ (if you don't use a docking station)

The scoop: D-Skin disc protectors, about $6 for a 5-pack, from D-Skin

What it does: The D-Skin is a thin, circular plastic protector that you can clip onto a CD or DVD and provide instant scratch protection. Once connected, the D-Skin stays on the disc, even while it is being played. The disc is readable through the protector so data quality is unaffected.

Why it's cool: Sometimes the easiest solution is the coolest. We normally don't think about disc protection, and then we get an inevitable scratch on a CD, DVD or video game disc so we must go find a scratch cleaner. With the D-Skin, we could add that layer of protection so we wouldn't get a scratch in the first place. We tried these on different video game systems, DVD players and computers, and the disc played correctly each time, with no interference from the D-Skin protector.

The D-Skin disc protectors will keep your CDs, DVDs and video game discs from getting scratched.

Grade: ★★★★

The scoop: Monstor 2G-byte USB drive, about $100, from US Modular

What it does: The Monstor is about the size of those old pagers/beepers (remember those?) and contains a hard drive with 2G bytes of capacity (a 4G-byte model is available for about $170). The drive connects via a USB 2.0 or 1.1 port to a PC and lets you transfer any type of file over to the device.

US Modular's USB 2.0 Monstor gives you 2G bytes of capacity on a flash drive for only $100.

Why it's cool: There's nothing earth-shattering here in terms of new features or abilities (there's no back-up software provided or anything like that). The cool part is its price — $100 for 2G bytes on a flash drive is pretty special — similar drives can cost up to $230 for 2G bytes. Having USB 2.0 on the drive also lets you transfer lots of files fast — we transferred 89 songs (about 300M bytes) to a USB 2.0-enabled laptop in less than 2 minutes.

Grade: ★★★½

Shaw can be reached at kshaw@nww.com.

The blade made for Linux. The tools to make it better.

Put a world leader in blades and Linux to work for you. More and more businesses are finding that HP BladeSystem servers are the tool their data center needs. One reason is that HP's blades are optimized for Linux. Not only do they ship with powerful software tools, like HP Systems Insight Manager™ and ProLiant Essentials, they also run key Linux apps from software partners like PeopleSoft and Oracle. And with powerful AMD Opteron™ Processors, you get maximum performance now as well as the flexibility to transition to 64-bit computing now or in the future. In short, HP offers you the advantages of blades, Linux and legendary HP reliability all in one neat, affordable package. Get more support, technology and advice from HP. So you can build the I.T. you need.

HP ProLiant BL25p Blade Server

HP ProLiant BL35p Blade Server

THE SOLUTIONS	THE BENEFITS[1]
• BL25p: 2 AMD Opteron™ Processors Model 200 (up to 2.60GHz) • BL35p: 2 AMD Opteron™ Processors Model 200 (2.40GHz) • BL25p: Up to 48 servers per rack • BL35p: Up to 96 servers per rack • HP Systems Insight Monoger™ for Web-bosed networked monogement through o single console • Rapid Deployment Pock for eose of deployment ond ongoing provisioning ond reprovisioning in Linux-mixed OS environments (optionol)	• Up to 23% sovings an ocquisition cost • Up to 23% less power consumption • Up to 93% fewer cobles • 43% less spoce needed for some number of processors • Hot-swappoble server design • Single interfoce for locol ond remote monagement of servers, storoge, softwore ond networking

Enhance your system. HP StorageWorks MSA1500cs

– Up to 24TB of capocity (96 250GB SATA drives) – Up to 16TB of capocity (300GB SCSI drives) – Ability to mix SCSI ond Seriol ATA enclosures for greoter flexibility – 2GB/1GB Fibre connections to host flexibility

Save up to $844 on the 4-hour response, 24-hour-a-day, 3-year warranty upgrade[2]

Save $1,744 when you purchase an HP BladeSystem enclosure and 8 BladeSystem Management Suite Licenses.[3]

CALL	**1-866-625-3909**
CLICK	**www.hp.com/go/bladesmag52**
CONTACT	**your local reseller**

AMD 64 Opteron

hp invent

1. Based on internal HP testing; compared to similarly configured HP1U, 2P server with SAN connectivity. For configurator, please visit: http://h30099.www3.hp.com/configurator/catalog-issipc.asp. 2. Offer valid through 7/31/05 on purchase of four-hour response, 24-hour-a-day, three-year warranty upgrade for MSA 1000 or MSA 1500 products. 3. Offer valid through 8/31/05 on purchase of HP BladeSystem enclosure and eight BladeSystem Management Suite licenses. Offers valid in U.S. only. Offers cannot be combined with any other offer or discount and are good while supplies last. See Web site for full details. Linux is a U.S. registered trademark of Linus Torvalds. Oracle is a registered U.S. trademark of Oracle Corporation, Redwood City, California. AMD, the AMD Arrow Logo, AMD Opteron and combinations thereof are trademarks of Advanced Micro Devices, Inc. ©2005 Hewlett-Packard Oevelopment Company, L.P.

ON TECHNOLOGY

John Gallant

Why complexity is the next killer app

One question I'm asked fairly often is: What's the next killer app?

The concept of the killer app has a powerful hold on our collective psychology. We want to believe that the entire market can be propelled forward by the next must-have technology that spawns a new generation of industry leaders and reshapes our lives. The spreadsheet, LANs, cell phones, e-mail, the Web and so on. Absent the next killer app, the market stagnates.

There's some truth to all this. PC sales were accelerated by the emergence of VisiCalc and 1-2-3. E-mail was a key driver in Internet adoption. But the role of the killer app also has been over-dramatized. No single product or technology moves a $1 trillion global marketplace buffeted by myriad macro- and microeconomic forces.

Yet the question persists and I always struggle to answer it. Hey, if I knew I'd start my own company and get rich. You think I want to be an editor forever? Sadly, like most people, I'm lousy at recognizing a killer app until well after it has proved its killer qualities. On occasion, I've thought a particular technology was a killer — can you say ATM? — only to watch it die a slow, painful death.

But today it dawned on me that there is a real killer app. It's called complexity.

That's a little play on words, actually.

You see, complexity is a *killer of applications*. We've built highly complex, fault-prone IT environments that cost more and more just to maintain each year. This complexity robs money that could be directed toward new applications that move our businesses forward. Complexity has made it more difficult for IT shops to embrace new technologies and new ideas. It's killing growth opportunities.

But complexity itself also represents a vast growth opportunity, and billions will be made helping users deal with it. It's a *true killer app*.

At the highest level, companies such as IBM are cashing in on concepts like on-demand or utility computing that promise to transform how we build and use infrastructure. At a point-product level, companies such as Egenera (blade servers) and VMware (server virtualization) are profiting from helping companies simplify certain facets of IT. Newly minted companies like Azul Systems (network-attached processing) and Cassatt (infrastructure virtualization) are being built on the mission of reducing complexity.

Complexity isn't sexy, and it isn't as much fun to talk about as the Web or IPTV. But if you're asking about the "next big thing," reducing complexity is the best answer I can think of.

— John Gallant
President and editorial director
jgallant@nww.com

opinions!

Switching sides

Regarding the story, "K-12 schools fight to stymie kid hackers" (www.nwfusion.com, DocFinder: 6722): It's refreshing to see school technology manager Lee Sleeper's comments that he's trying to get the kids who are doing the hacking to switch to "his side." Usually schools are so under-funded in the IT area that any help they get should be welcomed. The caveat is that the kids who break in should be counseled on why it's wrong. And who better to help close the holes than the ones who found them?

Dave Turner
IT manager
Wright Popcorn & Nut Company
San Francisco

On the block

Regarding Mark Gibbs' BackSpin column, "SBC makes DSL, er, exciting" (DocFinder: 6723): It was interesting to hear about a different side to the Port 25 blocking issue, but I have to disagree with Gibbs' conclusion. He writes that "[Port 25 blocking] also would hardly be a deterrent for serious spammers — they would just use a different port to transfer mail to a remote mail server."

That doesn't make sense because the target mail server would have to be listening on a non-standard port. The outgoing connection can be from any port you want — usually it's chosen randomly. It's the destination port that can't be changed (well, it can, but you sacrifice the ability to receive mail), and that's what SBC has started blocking. In short, what's being blocked isn't outgoing connections from Port 25, but to Port 25.

Now if Gibbs means that spammers would use a zombie to send mail to a server they already control (and then on to the target), or to another zombie on a network that doesn't block Port 25, I have to wonder what the advantage would be. Why not cut out the middleman and directly send to their own server or unblocked zombie?

Kelson Vibber
Irvine, Calif.

IT spouses in sync

I loved the story, "Of love and pagers: The life of married network pros" (DocFinder: 6724). Both my husband and I work in IT operations for the same 24/7 government organization, and it definitely has its upside and its downside. It seems like we speak another language and work in another world. Most non-IT spouses just don't understand when you get called at 2 a.m. with a problem, then have to work on it until it's resolved. I think it's important for those considering working in this industry to think about the personal side of their life, too.

Lisa Swanson
Senior systems software programmer
Hennepin County, IT Operations Network Services
Minneapolis

Not outfoxed

Regarding the story, "Should IE stay or should IE go?" (DocFinder: 6725): I feel compelled to respond to the statement that Active Server Pages are not available through Firefox. I develop Microsoft SQL-driven ASP applications for my company's inventory, asset and tech support tracking. I've had no problems reading or writing to the database or displaying the pages themselves using Firefox 1.0, 1.0.1 or 1.0.2.

Brian Norris
Owner
Integrated Technologies
Jacksonville, N.C.

E-mail letters to jdix@nww.com or send them to John Dix, editor in chief, Network World, 118 Turnpike Road, Southborough, MA 01772. Please include phone number and address for verification.

More online! **www.nwfusion.com** Find out what readers are saying about these and other topics. **DocFinder: 6721**

TOTALLY UNPLUGGED

Ira Brodsky

Looking beyond 3G wireless

Mobile-phone operators now must begin planning to meet potentially explosive demand for high-speed services such as mobile video and mobile e-mail.

The mobile phone industry finally is launching long-awaited 3G wireless services — and already a potentially huge problem looms. While 3G networks offer operators roughly three times the capacity of current 2G networks, 3G applications, such as mobile TV and mobile access to the Internet, enterprise networks and e-mail, guzzle more than 20 times the bandwidth of mainstay 2G applications such as voice and text messaging. 3G wireless devices — particularly handsets with high-resolution digital cameras and color displays — could spur demand far exceeding the capacity of mobile phone operators' 3G networks.

The industry is working to alleviate the problem by limiting and controlling demand and by applying the latest technology enhancements to squeeze out maximum performance from current 3G technologies. The industry believes it can constrain demand for 3G services, such as streaming media, through a combination of pricing, multicasting and downloading during off-peak hours. The bet is that most customers will be satisfied accessing professionally-created content from a menu.

Meanwhile, the industry continues to develop the leading 3G technologies, Wideband Code Division Multiple Access (WCDMA) and Evolution Data Optimized (EV-DO). The enhanced version of WCDMA is high-speed downlink packet access (HSDPA), which promises speeds up to 10M bit/sec. The enhanced EV-DO Rev A promises speeds up to 3.1M bit/sec and lower latency.

But what if users, given a taste of mobile broadband, insist on having it all — using their mobile phones and PC plug-in cards to upload and download whatever content they want, whenever they want it?

Rysavy Research (www.rysavy.com) studied this issue and concluded that mobile-phone operators now must begin planning to meet potentially explosive demand for high-speed services such as mobile video and mobile e-mail. The leading technology platform candidate for making this happen is multiple input/multiple output orthogonal frequency division multiplexing (MIMO) — also the core technology used by "pre-n" wireless LAN products that have demonstrated superior range than WLAN products based on today's standards. (See www.nwfusion.com, DocFinder: 6726).

The mobile phone industry is approaching a crucial juncture. Will it let new entrants, such as the WiMAX Forum, develop higher-capacity solutions, or will the industry take the bull by the horns and lead the development of technology to replace its current 3G standards?

It's a tough call. There's no doubt 3G wireless will be around for at least several years, and systems such as HSDPA and EV-DO Rev A will garner millions of satisfied subscribers. There's also no doubt 3G technology will continue to be enhanced. However, at some point it might make more sense to adopt a new technology platform that can carry the industry well beyond the capabilities of HSDPA and EV-DO Rev A.

The mobile phone industry must ensure it can meet users' growing appetite for bandwidth. This might require cannibalizing today's 3G technology. But it's better for an industry to cannibalize its own technology than let someone else do it.

Brodsky is president of Datacomm Research Co. of St. Louis. He can be reached at ibrodsky@datacommresearch.com.

REALITY CHECK

Thomas Nolle

Martin's FCC: More of the same?

Martin seems to have sent a signal with the FCC's recent ruling that the states cannot compel RBOCs to provide DSL to CLEC voice customers.

Kevin Martin's very public rift with then Federal Communications Commission Chairman Michael Powell in February 2003 over unbundling policy created a minor Beltway furor. Now that Martin has been named FCC chairman, the FCC's policy will change, right? Well, maybe not.

The cornerstone of the Powell/Martin feud was whether state public utility commissions could have a role in setting unbundling policy. Martin joined with the FCC Democrats Michael Copps and Jonathan Adelstein to push through an order that gave the states such a role, despite Powell's insistence that the order wouldn't survive an appeal. The Martin-brokered deal was seen as favorable to the competitive local exchange carriers (CLEC) and inter-exchange carriers, giving them a chance to lobby in the states for favorable unbundling treatment. But Powell was right; the D.C. Court of Appeals last summer vacated the order in a stinging rebuke. The new order, published late last year, was widely recognized as the death of unbundling.

This incident is important to the question of how Martin's elevation might affect telecom policy, particularly in unbundling. In its ruling last summer, the court said the states can't be given a role that by law is the FCC's. Martin signed off without comment on the order that resulted, perhaps using his silence to end the feud with Powell. He also might have sent his first signal on the policy direction his FCC will take.

Martin seems to have sent a signal with the FCC's recent ruling that the states cannot compel RBOCs to provide DSL to CLEC voice customers. Not only is that another nail in the coffin of unbundling-based competition, but it's also a further erosion of the states' role in the regulation of advanced services. Martin's partners in his February 2003 order, Copps and Adelstein, called the FCC's stance an application of the "heavy hammer of pre-emption" of the states. Martin was silent. What this almost certainly means is the FCC under Martin won't take a different position on unbundling than it had under Powell.

Martin may end up being a more effective advocate of the RBOC position than Powell, less for his beliefs than for his predisposition for coalition building and his greater decisiveness. Powell has been criticized for a more imperial style and for dawdling on key issues; Martin seems likely to be very different.

Then there are Martin's ties to the Bush administration. The administration has been widely criticized for lack of a strong telecom agenda, and some have advocated congressional action to rewrite key elements of the Telecom Act. It may well be that Martin's elevation to FCC chairman signals that the administration would prefer to manage telecom policy through the FCC, rather than through Congress.

The decision to push policy through the FCC has pros and cons. Congress, in its original writing of the Telecom Act in 1996, demonstrated the risk of having technical issues managed by legislation. Lobbying, poor understanding of the issues and simple blundering created a seven-year paralysis of broadband deployment. Using the FCC could prevent a recurrence of that tragedy. But the Telecom Act never explicitly mentions data services, the Internet, content, or other key issues. The FCC isn't a law-passing body; it's more like a court. Without a specific law to apply, the commission must resort to a form of judicial activism. That opens the risk of legal appeals and further confusion.

VoIP will be the litmus test for Martin's FCC. Last August, Martin was the only commissioner not to comment when the FCC issued its notice of proposed rule-making on the application of the Communications Assistance for Law Enforcement Act to VoIP and broadband access. The consolidation in the U.S. carrier market moves VoIP to a priority issue. Can Martin's FCC get the issue right and release a timely order?

Was Martin the heir to Powell all along, and watching his statements for political reasons? We'll likely find out by how the VoIP order goes.

Nolle is president of CIMI Corp., a technology assessment firm in Voorhees, N.J. He can be reached at (856) 753-0004 or tnolle@cimicorp.com.

Is your cell phone at risk?

Not at the moment, although new strains of viruses that infect smartphones pose yet another network security problem that you'll have to worry about in the future.

BY JASON MESERVE

Recent headlines such as "Cabir worm wriggles into U.S. mobile phones" conjure up the image of old tabloid headlines touting killer bees heading to the U.S. from South America. The latest buzz is that your cell phone could be infected with a nasty virus and you might not even know it.

Granted, your chances of infection are probably less than getting stung by killer bees, but mobile threats are only in their infancy and will continue to grow in sophistication, making the problem something IT staff should get on their radar early.

There are several mobile phone viruses in the wild at the moment, including Skulls, Cabir and Fontal (see graphic, page 50). And, like many PC-based viruses, each has its own set of variants aimed at keeping users and security vendors on their toes.

Skulls spreads by hiding in what looks like a harmless application for your mobile phone, be it a "theme" manager application or simple game. It replaces system icons with a picture of skull and cross bones and makes it difficult to access phone functions. Cabir variants — there are roughly 20 — use Bluetooth wireless technology to spread between phones in close proximity. And Commwarrior uses the Multimedia Message Service (MMS) to send infected files that look to be important security updates between devices. Commwarrior also will reset the device on the 14th day of the month, thus

www.nwfusion.com
More online
DocFinder:

SAVE $129

NetworkWorld®

Apply for a **FREE** Subscription

($129 value)

- 51 weekly issues
- Expert opinion
- Product tests and reviews
- 6 special issues

Subscribe today at my.nww.com

enter priority code B04A

SAVE $129

FREE

Subscribe today at

my.nww.com

Enter priority code B04A and SAVE $129

NetworkWorld®

How a cell phone virus spreads

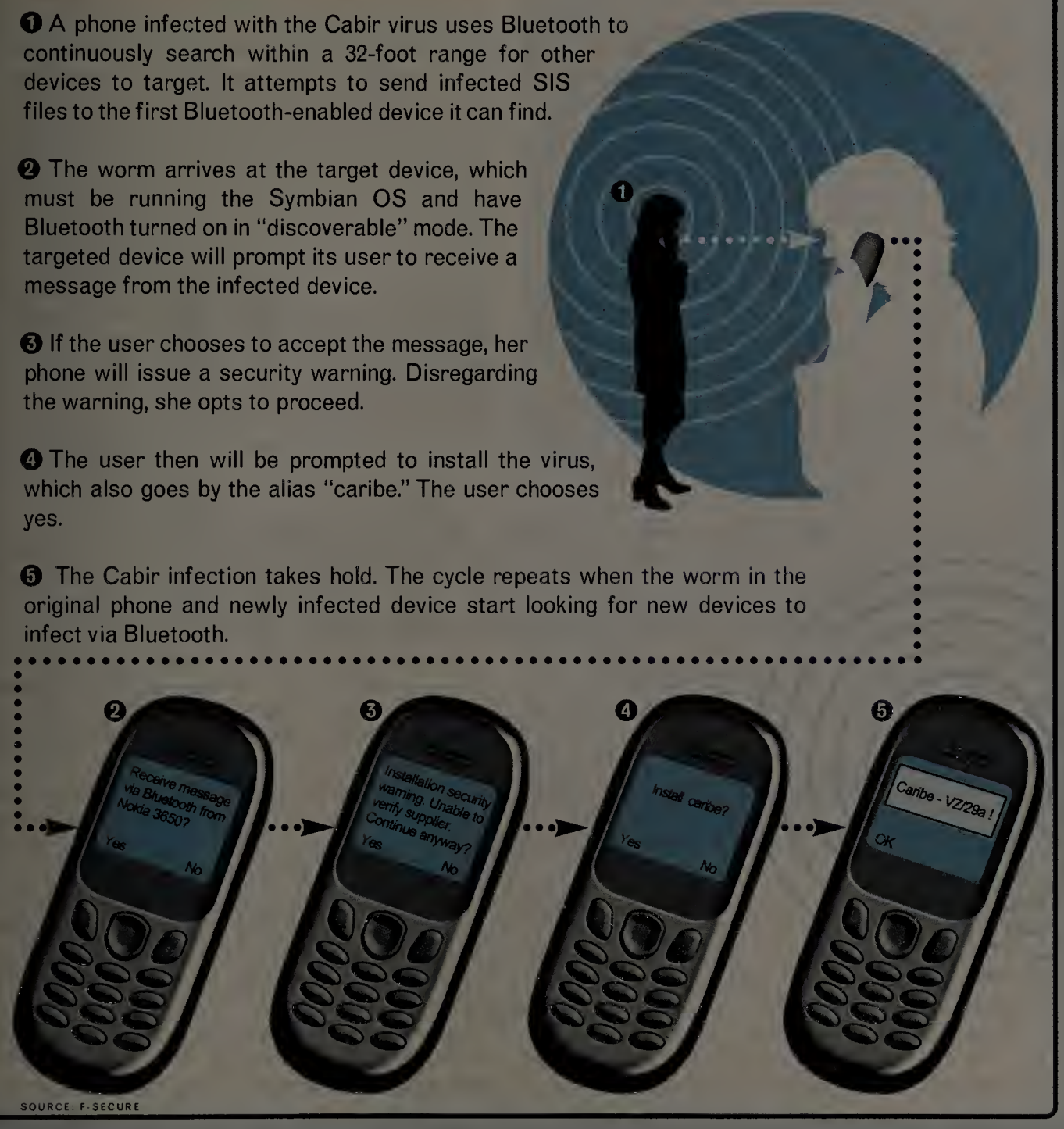
❶ A phone infected with the Cabir virus uses Bluetooth to continuously search within a 32-foot range for other devices to target. It attempts to send infected SIS files to the first Bluetooth-enabled device it can find.

❷ The worm arrives at the target device, which must be running the Symbian OS and have Bluetooth turned on in "discoverable" mode. The targeted device will prompt its user to receive a message from the infected device.

❸ If the user chooses to accept the message, her phone will issue a security warning. Disregarding the warning, she opts to proceed.

❹ The user then will be prompted to install the virus, which also goes by the alias "caribe." The user chooses yes.

❺ The Cabir infection takes hold. The cycle repeats when the worm in the original phone and newly infected device start looking for new devices to infect via Bluetooth.



SOURCE: F-SECURE

deleting all settings and data, if the virus is not removed in time.

Fortunately, the number of reported infections of each variant of Cabir, Commwarrior and Skulls fall in the 0-to-49 range, according to Symantec's virus threat database. Removal of the viruses is relatively easy, usually involving the deletion of infected files. In rare, more severe cases, the device might need to be reset to the original factory settings.

Vulnerable devices

The current slate of viruses all target the Nokia Series 60 smartphones running the Symbian operating system. A smartphone combines phone and PDA functions into one device. The good news is that 96% of the phones sold last year are not smartphones, use an operating system other than Symbian and are therefore completely immune to existing mobile threats.

Symbian holds the biggest share of the smartphone operating system market, with 13.65 million units shipped in 2004. Other operating systems such as palmOne and Windows Mobile accounted for another 6.6 million units, according to In-Stat/MDR. By comparison, the total number of worldwide mobile phones sold in 2004 was 678.9 million, says Neil Strother, a senior analyst at In-Stat.

Of the major wireless providers in the U.S., only T-Mobile and Cingular offer Symbian-based phones. Verizon Wireless and Sprint don't carry any Symbian devices.

Even if one does have a Nokia Series 60 device, it takes some effort to catch the virus. Unlike many of today's network-based worms that can spread between PCs and servers without any end user interaction, mobile viruses are far less sophisticated. With Cabir, users must have Bluetooth turned on and visible to nearby phones that are similarly equipped. An infected phone will constantly search for other Bluetooth devices to which it can pass its payload. The target machine will get a message asking the user to accept and install a SIS file (a Symbian file format) being transmitted via Bluetooth wireless. Users would have to accept both the transfer and installation of application to get infected.

Commwarrior works in a similar fashion, except it uses an MMS message that claims to be delivering an important Symbian security or application update, says Travis Witteveen, vice president of American operations at antivirus vendor F-Secure. Targeted users still have to accept the download and install the file to be infected. Commwarrior does add a bit of nastiness in that it embeds itself into application files on the device, making it more difficult to disinfect.

"Consumers have to go through hoops to get the virus," says Laurie Armstrong, a spokeswoman for Nokia, which has a large financial stake in Symbian. "These are not crazy, freely spreading viruses."

There's no inherent flaw — such as a buffer overflow or missing security feature — that virus code writers are exploiting in the Symbian operating system or Nokia's implementation of it. "The threats are targeting high-end phones that have fully functional operating systems and have the ability to download and install arbitrary applications," says Oliver Friedrichs, senior manager at Symantec Security Response.

Symbian offers a signed application service that digitally certifies the author of an application and that the application has not been changed since certification. When non-signed applications are installed, users get an additional "do you really want to do this?" warning.

"A Symbian-signed application [or any signed application in general] is a measure of certain standard of application," says Simon Garph, vice president of marketing at Symbian. "You know where it comes from and that it's been through a certain series of tests."

The mobile-oriented viruses are not designed to do much more than spread, although they might mess up a device enough that it has to be reset to the original factory settings or drain the battery because an infected unit constantly searches the airwaves for a new target.

"Right now they're more proof-of-concepts," Friedrichs says. "People are writing them to show that something can be done or that the phone platforms can be impacted by threats, just like the PC is."

The Windows operating system on the desktop offers enough low-hanging fruit for attackers to go after. The smartphone market has not reached critical mass yet, so it's not as attractive a target for the would-be virus writer. When a smartphone operating system grabs at least 20% of the

Protective action

There are a number of things mobile device users can do to ward off viruses:

• Beware of questionable downloads: When downloading a ringtone, game or business application for your device, make sure it comes from a trusted source. Nokia is working with Symbian to clarify the prompts given when a file is downloaded and installed to help users truly understand what they're doing.

• Get protection: For the truly paranoid, traditional PC anti-virus vendors are beginning to offer products for mobile devices. Symantec offers AntiVirus for Handhelds, McAfee sells VirusScan PDA, and F-Secure sells Mobile Anti-Virus to individuals and as a service via carriers. T-Mobile Germany and a Finnish operator resell the F-Secure system.

• Back it up: Red Bend Software is developing Firmware Over The Air technology that can be deployed in a wireless service provider's network and used to push updates to phones as new vulnerabilities are found. Many providers offer back-up technology for the phone, storing data centrally in case a device is compromised, lost or failed. FusionOne sells its back-up and self-destruct software to the service providers which in turn offer it to customers as a premium service. Verizon Wireless uses the FusionOne technology for its Backup Assistant offering.

— Jason Meserve

Staving off infection

Here's a sampling of current mobile threats, how they spread and how to remove the virus from devices.

Virus	How it's spread	What it does	How to remove it	No. of variants (as of April 6)
Cabir	Spreads via Bluetooth to nearby devices that are in "discoverable" mode. User has to accept the download and installation of the infected application.	No permanent damage, but can drain battery as worm seeks out new Bluetooth-enabled targets.	Removal tools are available from anti-virus vendors.	21
Commwarrior	Spreads via Bluetooth and MMS messages, claiming to be an important application or Symbian OS security update. User still has to accept file transfer and install.	No permanent damage. It can drain battery as it sends MMS messages to contacts in the device's address book and looks for targets via Bluetooth.	Removal tools are available from anti-virus vendors.	1
Drever	User downloads/installs malicious "antivirus.sis" file.	It disables Simworks and Kaspersky anti-virus software for Symbian. Needs to be reinstalled.	Use Application Manager to uninstall "antivirus.sis."	3
Fontal	Malicious SIS file that user downloads from peer-to-peer or other site.	Installs a corrupted application on Nokia Series 60 phones, causing them to lock.	Restore phone to original settings, erasing all data.	1
Locknut	Another malicious SIS file that a user has to download and install.	Virus can cause problems with Symbian ROM, making phone lock.	Removal tools are available from anti-virus vendors.	2
Mabir	A new version of Cabir that spreads by sending a SIS file via Bluetooth and MMS; virus replies to incoming messages.	No permanent damage, but could drain battery.	Removal tools are available from anti-virus vendors.	1
Skulls	User downloads a malicious SIS file. File looks like a theme manager or some other handy application.	Replaces application icons with skull and crossbones; hinders access to applications.	Removal tools are available from anti-virus vendors.	8

market, it will become a better target, says Patrick Hinojosa, CTO at anti-virus vendor Panda Software.

"How many Amiga viruses are there? You could write a virus for it, but how is it going to spread [efficiently]?" Hinojosa asks.

Although more smartphone operating systems could be similarly susceptible to such worms, none have been found yet.

"I am not worried about it right now," says Roald Haugan, global telecom manager for Artesyn Technologies, a power conversion equipment maker in Boca Raton, Fla. "I've got other balls on the court to worry about."

Haugan says that only a few his users actually have Bluetooth technology running — mostly Research in Motion BlackBerry devices.

Future threat

Although today's mobile virus threat might not be much of a worry — the equivalent of the early "Stoned" virus that infected DOS-based PCs — the threat will grow as the devices become more PC-like.

Smartphones do have an upward growth path over the next few years. "In five years, we won't think of it as a 'smartphone,'" Strother says. "The phone in 2010 will be pretty sophisticated and handle a lot of data and heavy traffic."

Caleb Sima, founder and CTO of SPI Dynamics in Atlanta, sees a number of potential issues as smartphone technology lands in the hands of more mainstream users.

Bluetooth is a security challenge on a few fronts. For one, an attacker doesn't have to be that close to its target. A typical Bluetooth signal can travel about 32 feet, but there are people who have developed antennas to increase the range to almost 1 mile. That signal can be used to gather information from a phone (a practice known as bluesnarfing), make calls on the device or to transmit malicious code — as Cabir does.

"You could sit in an airport or mall with a laptop and pick up tons of stuff and junk from people's cell phones," Sima says. Vendors now are disabling Bluetooth by default, but as more devices — such as cars — use the technology, it will need to be enabled more often, opening another attack vector.

The mobile device might even carry a virus back to a PC when the two devices synchronize. A road warrior may pick up a virus outside a network perimeter on his mobile device, bring it back inside the firewall and synchronize with his work machine, spreading the virus on the LAN. The potential of this is more limited because anti-virus software on the PC should catch the infected file before it wreaks havoc.

Sima says he's heard rumblings of a Trojan horse application that could be installed on a device through memory cards, infrared file transfer or synchronization. An attacker could send a special text message to the infected phone, signaling the Trojan to send the last 5 minutes of recorded phone conversation. "It could send it as a message attachment without the user knowing," Sima says.

Buffer overflows, a common problem with PC-based applications in which too much data is received and not properly handled, let an attacker ultimately run his own code on the affected machine. This could crop up in the mobile world. There's currently not enough of an incentive (financial or otherwise) to look for such issues in a mobile application, but there will be when consumers start using their phones to pay for items at a vending machine or to extract cash from an ATM, as they do in Japan.

It was a buffer overflow exploit that led to one of the hacks of T-Mobile accounts. However, the phone was not the problem. A non-patched Web application server looked to be the weak point, Sima says.

Even today, one could use text messaging to launch a denial-of-service attack against a phone, Sima says. An attacker could run a program on his PC that sends thousands of text messages to a phone number. The flood would render the phone's interface useless. Even if the phone doesn't freeze up, many service providers limit the number of text messages an account holder can send and receive before incurring extra charges. Thousands of text messages could result in an unexpectedly large bill for the victim.

F-Secure's Witteveen worries that as more people become dependent on their mobile phones as their only phone, 911 emergency calls could become a problem should a phone be attacked.

There's also the issue of fixing devices that have been compromised. "We need to have a centralized service provider take care of problems," he says. "An 18-year-old working at the phone kiosk at the mall would get bombarded if anything big hit."

However, mobile devices will continue to flourish despite the increased risk of future infection. "As the handsets get more sophisticated and computer-like there is a greater potential, but that hasn't stopped the computer business from expanding to the masses," Strother says. These threats "will be another modern day digital hassle that people will have to live with." ■

Spam that follows you and makes you pay

Nothing more annoying than receiving unwanted spam? How about getting your phone bill filled with unwanted charges for spam that you're actually trying to pay for?

Wireless spam is starting to appear as text messages on cell phone users' small screens. Like wireless viruses, this nuisance doesn't yet compare to the viruses and unwanted mail that strike PCs, but experts say the problem will escalate quickly.

"The tolerance level is much lower for spam on wireless phones, so this is a problem that will [grow] even faster than e-mail," says Sara Radicati, an analyst with The Radicati Group.

Text-messaging spam is particularly annoying because, per service agreements with their carriers, subscribers likely pay a few cents to receive a text message. And these messages usually cause the phone to beep when they arrive. "It drives me crazy when my BlackBerry's alert goes off and it's junk mail," says Frank Gillman, director of technology with Allen Matkins, who manages at least 250 cell phones for the law firm.

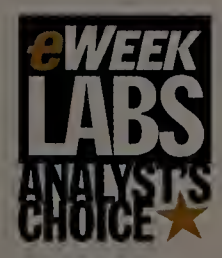
Unlike e-mail spam, there aren't applications on the market to protect users from these messages; because text messages are delivered through the carrier's wireless network, it's up to the carrier to stop spam before it gets to subscribers. Most carriers are taking such steps; Verizon Wireless has spam filters installed on its network and has prosecuted some text-messaging spammers — a step the company believes will act as a deterrent. But given how easy it is to text message people you don't know (a 10-digit cell phone number at the wireless operator's domain, for example 1234567890@operator.com), it isn't hard to believe text messaging could be the next fertile ground for spammers.

— Cara Garretson

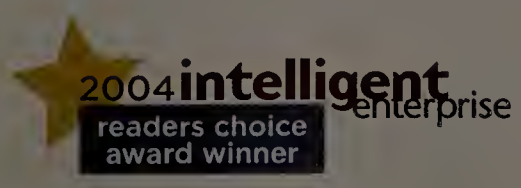
Oracle Business Integration

Best in Class Integration

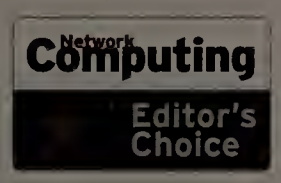
Oracle BPEL Process Manager 10*g*
August 2004



Oracle Application Server 10*g*
July 5, 2004



Oracle Customer Data Hub
September 4, 2004



Oracle Application Server Portal 10*g*
May 13, 2004

Integrate all your business information.

ORACLE®

oracle.com/integration
or call 1.800.633.0641

Copyright © 2005, Oracle. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

CLEAR CHOICE TEST

IP telephony systems

Aastra offers plug-and-play VoIP

■ BY EDWIN MIER AND DAVID MIER, NETWORK WORLD LAB ALLIANCE

Aastra Technologies bills its VentureIP package as an enterprise-class, peer-to-peer, IP-based phone system that automatically configures itself — no complex setup or centralized server equipment required.

In our Clear Choice test of the VentureIP system, we found that most of these claims were true. There is no central PBX or server, a full spectrum of enterprise telephony features is supported, reliability and call quality are good, and the auto-configuration of the system is impressive. On the downside — at least if you are considering an enterprise deployment — the system now only runs within one IP subnet, and there is no attendant console.

Small to midsize businesses could see cost savings in several ways. First, the typical $1,000 per day for an IP-PBX installation, training and phone-cable testing is avoided. Second, with the plug-and-play and auto-configuration features, specialized administration costs are eliminated. Finally, a 50-station price for this package is less than $400 per user, 20% to 40% less than typical, low-end IP PBXs.

Using Category-5 10/100M bit/sec LAN connections, you attach VentureIP 480i telephones and VentureIP Gateway units to your switched network. You then plug up to four analog central office trunks into each gateway, turn everything on and step back.

In our tests, everything booted up OK, but the phones wouldn't let calls through. We needed to turn off the Internet Group Management Protocol (IGMP) Snooping feature in our Layer 3 Extreme Summit switch, which was hindering the passage of IP-multicast traffic. The system uses IP-multicast to locate, update and configure itself. Aastra says its auto-configuration process has been successfully tested on Layer 2 switches from D-Link Systems, Linksys, Netgear and SMC.

With IGMP Snooping turned off, the system's auto-configuration worked flawlessly. IP addresses and extension numbers were derived and assigned; the auto-attendant, voice mail and phone directory configured. Users could place and receive local and remote calls, get and retrieve voice mail, and use the full spectrum of telephony features (forward, hold and transfer).

The target installation is 50 stations with up to 200 extensions supported per system. Because more than 90% of PBX installations have 100 or fewer stations, the VentureIP would seem to fit well in this lower-end, phone-system marketplace.

The current release (2.8.2) requires that all VentureIP phone sets and gateways be contained within the same IP subnet. Aastra says it plans to add the ability to work across IP-routed links later this year. But until then, this IP-based system cannot take advantage of distance insensitivity, a hallmark of IP telephony through which a system's call control is distributed across multiple remote sites.

A plus for the VentureIP system is its standards support. A unique combination of Layer-2 discovery tools is used for all the auto-deployment features, but call control is Session Initiation Protocol (SIP)-based. Each phone incorporates full SIP endpoint functionality and the smarts to keep track of every other phone. Each phone handles and stores its own voice mail, up to 20 minutes of total storage. If a phone is unavailable, a caller can still leave voice mail for that extension. Another phone with extra storage capacity will accept the unavailable phone's voice mail messages and deliver the messages when the phone is available.

The phone sets are all powered by 802.3af-based Power over Ethernet. If your switches don't deliver this, Aastra offers small 802.3af power-insertion units.

As for classic telephony features, we exercised voice mail, three-party conferencing, forwarding and call transfer, hold, directory, redial, multiple call appearances, do-not-disturb and music-on-hold.

However, we found that a few features documented by the vendor were still not available, including the ability to tag VoIP traffic for a particular virtual LAN (for QoS handling) and the ability to send voice mail as e-mail attachments.

There are other fairly common options that competitive low-end IP-PBX makers offer that Aastra currently does not, including a softphone application, a subsystem for interactive voice response/voice recognition, call/contact center, text-to-speech, collaboration or multimedia. Also absent is an attendant console, hard or soft, which we feel is necessary in systems with more than 20 stations.

One key advanced feature that is supported is encrypted VoIP streams. We confirmed this system's encryption of voice-payload, real-time, transport protocol streams prevents VoIP conversations from being deciphered or replayed.

If an administrator wants to tailor the system, he can define many of the key parameters (IP addresses, DHCP and extension numbers) only via the phone buttons and display screen on the VentureIP. There is also Web browser access to each phone, but that only lets you change a handful of settings for that phone and user.

As more elaborate features are added to the system, management will need to expand. There currently is no real-time monitoring or activity reporting. There is no bandwidth management either, because currently only one vocoder, G.729a, is supported, and IP-WAN links are not.

The system gets high marks for performance. Because IP-call connectivity now is not supported over wide-area links, call quality and call setup times were all always good. We measured typical end-to-end latency for VoIP calls at just 69 millisec, virtually imperceptible to callers.

Aastra's VentureIP package delivers the classic telephony features most users would expect in a low-end phone system. While the vendor needs to shore up some of its IP-telephony features, his peer-to-peer phone system is sound, and it should be considered a viable, low-end, IP-telephony contender.

Edwin Mier is president and David Mier is lab manager at Miercom, a product testing firm in East Windsor, N.J. They can be reached at ed@miercom.com and dmier @miercom.com.

How We Did It

Aastra's VentureIP system was deployed over a network of Extreme Networks' Summit switches. Because the VentureIP phones now do not work across routed IP links, we set up the Summit switches with Layer 2 switching only enabled and Layer 3 IP-routing disabled.

Telephony features — forwarding, conferencing and the like — were tested with the three phone sets the vendor provided in the lab and with remote phones via a PSTN analog FXO trunk connected to the VentureIP Gateway. The remote phones were TDM sets on a Lucent/Avaya Partner PBX.

We manually assessed call quality. Latency was measured by injecting a tone into one phone's handset, and clocking the one-way delay until arrival of the tone at another phone's handset connection.

Net Results

VentureIP 480i telephone and VentureIP Gateway — OVERALL RATING 4.0

Company: Aastra Technologies, www.aastra.com **Cost:** $379 per IP telephone; $289 per four-port IP-analog gateway. **Pros:** Plug-and-play for the most part; no central-site servers or PBX; standards-based SIP; 802.3af power; intuitive operation. **Cons:** Currently limited to a single IP subnet; some IP telephony features not yet supported; needs an attendant console.

The breakdown

Installation and configuration 25%	4.5
Features 25%	3.5
Management & administration 25%	3.5
Performance 25%	4.5
TOTAL SCORE	4.0

Scoring Key: 5: Exceptional; 4: Very good; 3: Average; 2: Below average; 1: Consistently subpar

More online!

For weekly updates on VoIP, sign up for our free Convergence newsletter.

DocFinder: 6731

NW Lab Alliance

Miercom also is a member of the Network World Lab Alliance, a cooperative of the premier testers in the network industry, each bringing to bear years of practical experience on every test. For more Lab Alliance information, including what it takes to become a partner, go to www.nwfusion.com/alliance.

Preventing identity mega-theft

■ BY ANDREAS ANTONOPOULOS

While companies say they collect information on consumers to better serve them, the worst disservice they can do is to inadvertently expose customers' private information. Every few weeks it seems that another huge number of credit cards or Social Security numbers is stolen from a database. Consumers are understandably furious. They can buy shredders to make sure they're not putting their private data out there, but what can they do when their data is mixed with millions of records in a poorly secured database?

There are several things data center managers can do to protect customers' identities. The simplest solution is to not collect information that you don't really need. If you want to be able to find a customer quickly, a phone number will often suffice. Pet's names, high school names and favorite colors can be used instead of birthdates or mother's maiden names. No database is guaranteed to be secure, no matter how many security tools or precautions you use. Assess the risk of storing each piece of data against the benefits, and try to find less risky alternatives.

If you must store Social Security numbers for verification, then perhaps store it as a one-way-hash. Instead of storing 123-12-1234, convert it to a one-way-hash of 23F5A1C2 and store that instead. If you need to find someone, ask for their Social Security numbers, convert it (once) and search on the index of one-way-hashes. If you need to verify their Social Security numbers, ask for it and then just check if its one-way-hash matches 23F5A1C2. Do you ever need to retrieve the actual Social Security number itself, or are you only using it as an index key?

Encrypting data in a database, unlike one-way-hashes, can involve some significant computational overhead. Furthermore, it requires careful key management to avoid data loss. If you want to pursue such an approach, it is best to use a front-end encryption device that transparently encrypts and decrypts. Beyond improved performance, hardware-based database encryption products such as Ingrian's DataSecure appliance provide key management and recovery.

Finally, if you can't protect each record you can at least protect against mega-theft by fine-tuning the database permissions. A database access control and monitoring product such as Guardium's SQLGuard can filter and selectively block SQL statements that do not match a pre-defined policy, or detect transgressions and alert your security team. Even database administrators don't often need to do "SELECT * from CREDIT_CARDS".

Bottom line: Avoid storing data you don't really need to store, use one-way-hashes to protect data, encrypt where appropriate and filter SQL with policies. These approaches are much preferable to infuriating your customers and being "named and shamed" in the press.

Antonopoulos is principal research analyst at Nemertes Research. He can be reached at andreas@nemertes.com

AuditWizard V6 - Simply Effective

No other software makes auditing your network as quick and easy as AuditWizard™.

Install, then sit back and let AuditWizard™ do all the complicated stuff. AuditWizard™ will automatically discover all of the PCs connected to your network then conduct a comprehensive software and hardware audit of each one - without any user intervention from you.

So when the boss asks for that Software License Compliance Report - you're good to go...

...if only everything in life was as simple to use as AuditWizard™

For more information telephone 813 319 1390
or email sales@auditwizard.com

Download a FREE trial today! **www.auditwizard.com**

LAYTON Technology

In your in-box

Sign up for this or any of *Network World's* many other e-mail newsletters.

www.nwfusion.com
DocFinder: 2778

www.TheMotherOfAllAlarmStorms.com

A fun and informative site for anyone who's ever been in the data center when the bells start ringing.

Securely access and control your IT infrastructure with solutions that simplify and accelerate incident response, service restoration, problem diagnosis and repair – helping to reduce complexity, MTTR and downtime, while improving productivity, flexibility and ROI.

Raritan®

When you're ready to take control.™

Management

Strategies

...VELOPMENT
...ANAGEMENT
... JUSTIFICATION

The IT apprentice

The state of North Dakota taps training program for help with network overhaul.

■ BY LINDA LEUNG

There's no better way to get new skills than rolling up your sleeves and immersing yourself in a brand-new role. Brandy Peterson, who for the past four and a half years has worked as an administrative assistant within the telecom division of the North Dakota state government's IT department in Bismarck, has just dived into the state's multimillion-dollar network replacement program as a project manager.

Peterson, whose supervisor had pinpointed project management as a future career path for her, is among the first of a group of state IT employees who will be trained under the National IT Apprenticeship System (NITAS). The program, a partnership between the U.S. Department of Labor and the CompTIA trade association, is being rolled out across the country after an 18-month beta test initiative.

For the next year, Peterson will shadow her mentor, Dirk Huggett IT business analyst within the state's policy and planning division, as he oversees the project to overhaul the state's backbone infrastructure. "I will be getting a lot of hands-on experience. Being tied to a mentor, I will have someone to bounce ideas, which is good," Peterson says. She began her journey into project management when the 18-month-long network project was launched in March.

The project, called STAGEnet Infrastructure Services, will replace the state's ATM network. The state hopes to convert to a high-speed WAN using lambda switching technology that will carry a range of applications, including human resources and ERP software, for state government offices, K-12 schools and universities.

According to Huggett, the value of the total contract for all vendors involved will be between $35 million and $50 million. RFPs will be issued in early July, with vendor contracts to be signed in September and implementation to be completed in July 2006, Huggett says.

On-the-job training

NITAS students are assigned an in-house or external skills validation consultant or mentor for hands-on learning of industry-developed and validated competencies, and receive classroom training. CompTIA divided IT roles into several tracks including security, networking and and project management — Peterson's track.

There are three levels to the project management track, and the difference depends on the size and scope of the project in which the students will be involved. Even though North Dakota's project is considered a Level 3 initiative — the highest level — Peterson will be limited to the entry-level Level 1 duties, which include initiating, scoping and planning a project; developing the project schedule; determining the project cost and acquiring the resources.

Within these duties are 30 project management competencies or skills that Peterson will need to get under her belt. Each competency has to be validated by Huggett, who confirms that she has applied each skill in her new role before she can move on. Peterson will be given a small portion of the project to manage.

"Brandy will be involved in writing the business case, reviewing documents and deliverables, and will be in charge of the organizational aspects. She will help develop part of the project plan and will also take the lead in some of the post-implementation processes," Huggett says. Those processes will include developing and managing team and end-user surveys, and facilitating some of the lessons learned in meetings.

Although Peterson is not a technologist, she says she is looking to hone her organizational skills that will help keep the project on track and on budget. Indeed, the NITAS program is applicable to everyone, from IT novices to IT professionals looking to gain skills in new areas of the industry or advance their knowledge within their specific fields, according to Neill Hopkins, CompTIA vice president of skills development.

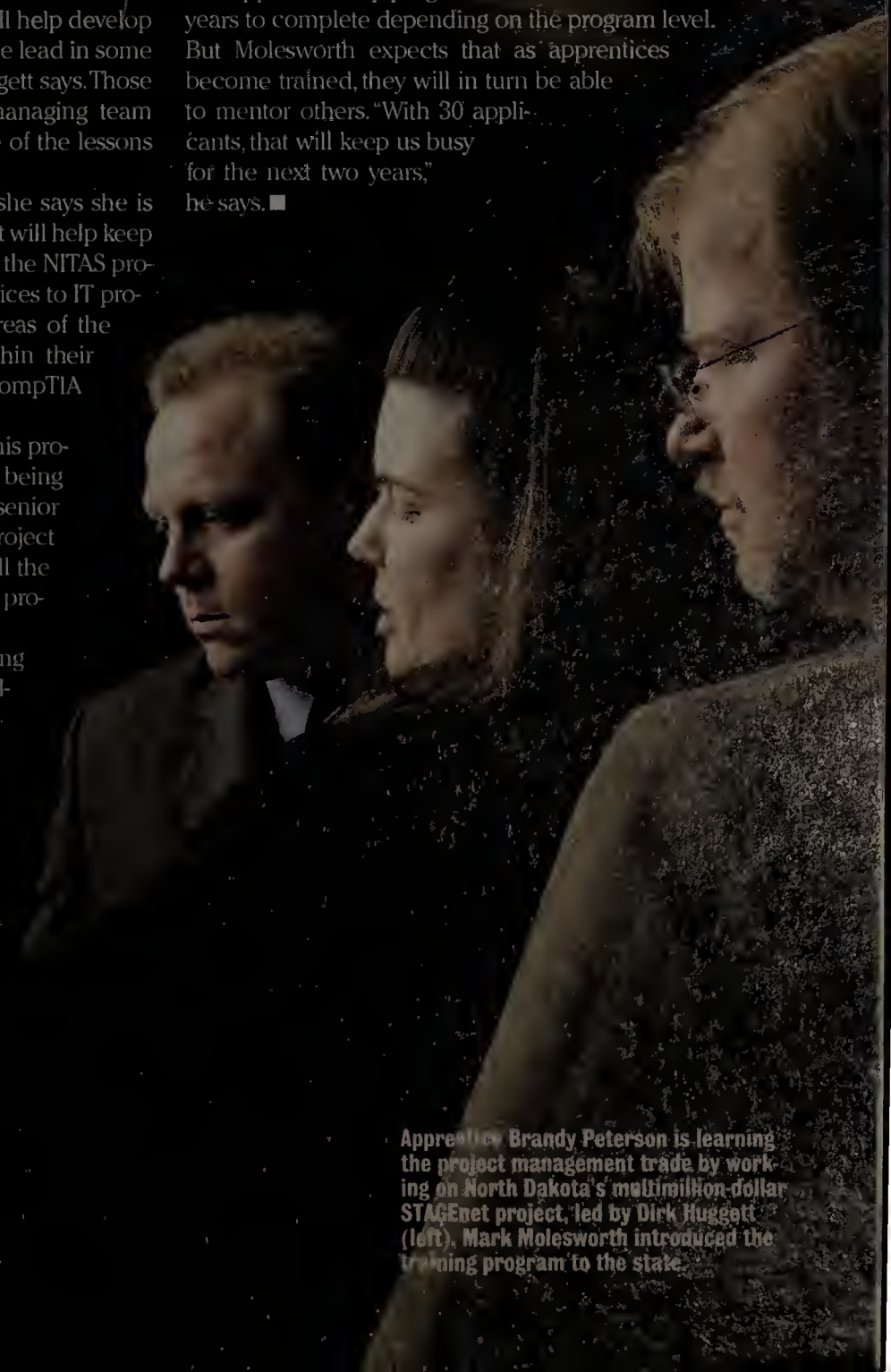
To be a mentor, Huggett also has to have his project management skills validated. This is being done by peer review with the state's other senior project managers, including Enterprise Project Manager Mark Molesworth, who oversees all the state's IT projects and introduced the NITAS program into the organization.

"Giving up control and turning something over to the apprentice will be the main challenges" of being a mentor, Huggett says. "The rest isn't difficult; it's a matter of taking the time to spend with the apprentice. It's the apprentice's responsibility to push forward to the next skill competency. My responsibility as a mentor is to review and offer constructive criticism."

Molesworth says he introduced NITAS to the state because it lacked a skills validation aspect in its project management training programs. The state mandates that IT projects that cost more than $250,000 over two years, or $500,000 during the life of the contract, require project oversight. Molesworth says the state averages about 18 to 24 projects at any given time that fit that criteria. Producing well-rounded project managers is the goal of the state's NITAS program. "Certifications and education show that you know how to do something, but NITAS shows you can do the job," he says.

After presenting the NITAS initiative to some 50 potential candidates, Molesworth received 30 applicants for the apprenticeship program — double the number he expected. Molesworth says he would like to see everyone through the program but initially he is limited by the number — seven so far — of senior IT staff who have agreed to become mentors.

The state has limited mentors to one apprentice each, and apprenticeship programs take between one and two years to complete depending on the program level. But Molesworth expects that as apprentices become trained, they will in turn be able to mentor others. "With 30 applicants, that will keep us busy for the next two years," he says. ■



Apprentice Brandy Peterson is learning the project management trade by working on North Dakota's multimillion-dollar STAGEnet project, led by Dirk Huggett (left). Mark Molesworth introduced the training program to the state.

SERVERS WITHIN YOUR REACH FROM ANYWHERE

LOCAL OR REMOTE SERVER MANAGEMENT SOLUTIONS

UltraMatrix™ Remote

KVM OVER IP

MATRIX KVM SWITCH WITH INTEGRATED REMOTE ACCESS OVER IP

- System-wide connectivity locally or over IP from any location worldwide
- Connects 1,000 computers to up to 256 user stations
- Supports PC, Sun, Apple, USB, UNIX, and serial devices
- High quality video up to 1280 x 1024
- Secure encrypted operation with login and computer access control
- Scaling, scrolling, and auto-size features
- View real-time 4 computer connections using the quad-screen mode

The UltraMatrix Remote represents the next generation in KVM switches. It not only provides a comprehensive solution for remote server console access, this access can be local or from any workstation on your network over IP.

UltraMatrix™ E-series

KVM SWITCH

PROFESSIONAL MULTI-USER KVM SWITCH 2 - 4 KVM STATIONS TO 1,000s OF COMPUTERS

- PC or multi-platform (PC/Unix, Sun, Apple, ot ers
- On-screen menu informs you of connection statu between units in an expanded system
- Powerful, expandable, low cost
- No need to power down most servers to install
- Security features prevent unauthorized access
- Free lifetime upgrade of firmware
- Video resolution up to 1600 x 1280
- Available in several models
- Easy to expand

The UltraMatrix E-Series represents the latest in KVM matrix switch technolog, at an affordable price. The E-Series allows you to connect up to 256 users to as many as 1,000 computers. The UltraMatrix E-Series is available in several sizes: 2x4, 2x8, 2x16, 4x4, 4x8, 4x16, 1x8, and 1x16 and either PC or multi- platform.

KVM RACK DRAWER WITH KVM SWITCH OPTION

The RackView offers the latest, most efficient way to organize and streamline your server rooms and multiple computers. The RackView is a rack mountable KVM drawer neatly fitted in a compact pull-out drawer. This easy-glide KVM drawer contains a high-resolution TFT/LCD monitor, a tactile keyboard, and a high-resolution touchpad or optical mouse.

RackView Fold-Forward | RackView Fold-Back | RackView LCD Monitor | RackView Keyboard

ROSE US +281 933 7673
ROSE EUROPE +44 (0) 1264 850574
ROSE Asia +65 6324 2322
ROSE Australia +617 3388 1540

800-333-9343
WWW.ROSE.COM

ROSE ELECTRONICS

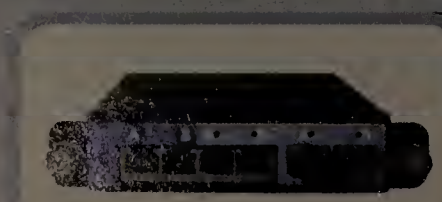
networkTAPs.com

TAP into Performance

Monitor mission-critical links with the latest technology through new *n*TAPs

Stop jeopardizing network performance and risking costly downtime. Be confident you have maximum visibility into your full-duplex links by configuring an *n*TAP solution that fits your network and budget. Visit **www.networkTAPs.com/visibility** today.

Ethernet Copper *n*TAP
For copper-to-copper connections
Choose your speed:
10/100 ..... $395
10/100/1000 ..... $995



10/100/1000 Conversion *n*TAP
Copper input with copper or fiber output options
Choose your analysis output:
SX $1,995
LX $1,995

Optical Fiber *n*TAP
Multiple split ratios
Choose your port density:
Single channel $395
Four channel $1,795
Six channel $2,395

To learn more about how *n*TAPs can boost your network visibility and which configuration option is best for you, go to **www.networkTAPs.com/visibility** or call 866-GET-*n*TAP today.
Free overnight delivery.*

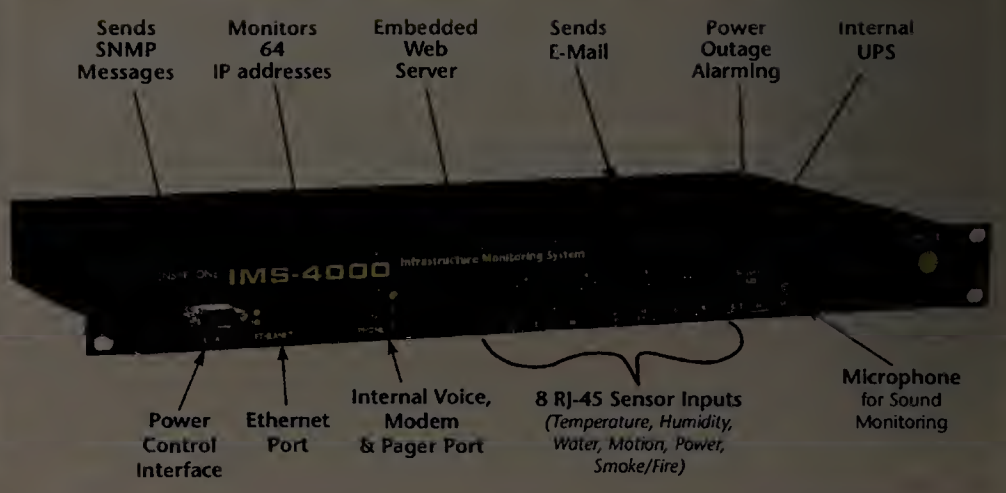
FC CE *Free overnight delivery on all U.S. orders over $300.00 confirmed before 12 pm CST.
*n*TAP and the *n*TAP logo are trademarks or registered trademarks of Network Instruments, LLC

*n*TAP™

SENSAPHONE

IMS-4000

IMS SOLUTION



BE NOTIFIED BEFORE CRITICAL EVENTS TURN INTO DISASTER!

- Eight environment inputs
- Power sensing
- Monitors 64 IP addresses
- Send alerts to 64 people
- 8 methods of contact
- Calendar scheduling
- Expands to 256 sensors
- Remote power control
- Optional camera

The Sensaphone IMS-4000 Infrastructure Monitoring System monitors critical environmental and network elements in your server room, data center, or telecomm installation and reports to you instantly when events threaten your infrastructure. The IMS-4000 keeps watch so you don't have to. See these features and more on the web at www.ims-4000.com

Tel: 877-373-2700
www.ims-4000.com

Phonetics, Inc.
901 Tryens Road
Aston, PA 19014

Cyclades
KVM over IP

Enjoy the magic

Secure KVM over IP switch

Web-based access

Centralized system management

Remote incident resolution

Cyclades AlterPath™ KVM/net offers a unique set of features:

- Server-based authentication
  (NT domain, LDAP, Secure ID, RADIUS, TACACS+)
- 16 and 32 port models
- CAT5 cabling up to 500 feet
- User access logging
- System event syslog
- Integrated power management

We've worked our magic.
Now you can work yours.

Over 85% of Fortune 100 choose Cyclades.

www.cyclades.com/nw

1.888.cyclades · sales@cyclades.com

cyclades

© 2004 Cyclades Corporation. All rights reserved. All other trademarks and product images are propert[illegible] of their respective owners. Product [illegible]

Overheated?

Plug In The Simple Solution.

MovinCool spot air conditioners are the answer to your overheating problems. Just roll it in. Plug it in. Turn it on. It's that simple.

- ▶Up to 60,000 Btu/h of cooling power right where and when you need it
- ▶Protects against data loss and equipment failure
- ▶#1 in portable air conditioning for over 30 years
- ▶The only portable air conditioner ETL-verified for performance

MOVINCOOL®

THE #1 PORTABLE SPOT COOLING SOLUTION

800-264-9573 or visit www.movincool.com

©2005 DENSO Sales California, Inc. MovinCool, SpotCool and Office Pro are registered trademarks of DENSO Corporation.

The Truth about Secure-Out-Of-Band

Terminal server vendors, who proclaim that they have Secure Out Of Band products, rely on RADIUS, TACACS+ and other in-band protocols to provide security. By inference, they imply they secure out of band access when, in fact, they offer only network security which conflicts with out of band access.

A true Secure Out of Band Management solution should provide strong security without reliance upon network-based protocols.

CDI offers:

- Hardware encryption over dial-up and network connections
- RSA certified SecurID authentication without a network.
- Patented central management of all remote devices
- Full NIST, FIPS 140-2 certifications
- Remote Power control
- Homologous world-wide approved internal modems

CDI has been building encryption equipment for over fifteen years. Our customers and partners include major financial institutions, government agencies, major telcos, utilities, and the United States military.

Communication Devices Inc.
www.outofbandmanagement.com

How Do You Distribute 20,000 Watts in Your Cabinet?

Sentry CDU Cabinet Power Distribution

- High-Density Equipment Cabient Power Distribution «
- 84-Outlet Receptacles «
- 20,000 Watt 3-Phase Power Distribution Model «
- 10,000 Watt 208 VAC Power Distribution Model «
- True RMS Power Monitoring per Branch Circuit « Local: Digital Displays, Remote: via Interface
- Input Power Monitoring Facilitates Load Balancing «
- Web Interface «
- SNMP, MIB & Traps «
- Internal Temperature & Humidity Probes «
- Receptacles by Branch Circuit/Electrical « Phase for Easy Identification
- Simplifying Cabinet Installation «

Technology, Inc. Sentry is a trademark of Server Technology, Inc

Server Technology

Solutions for the Data Center Equipment Cabinet

Power demands from today's new servers require greater power distribution in the equipment cabinet. The Sentry CDU distributes power for up to 42 dual-power 1U servers in one enclosure. Single-phase or 3-phase input with 110 VAC, 208 VAC or mixed 110/208 VAC single-phase outlet receptacles.

Server Technology, Inc.
1040 Sandhill Drive
Reno, NV 89521-USA

toll free +1.800.835.1515
tel +1.775.284.2000
fax +1.775.284.2065

www.servertech.com
sales@servertech.com

SUN MICROSYSTEMS · COBALT · CISCO SYSTEMS

SUN COBALT CISCO

Tel: 408.727.1122
Fax: 408.727.8002

3431 DE LA CRUZ BLVD.
WWW.RECURRENT.COM

renewed
USED
buy Sell
LEASE

VISA MasterCard AMERICAN EXPRESS

ReCURRENt
technologies, inc.

SANTA CLARA, CA 95054
INFO@RECURRENT.COM

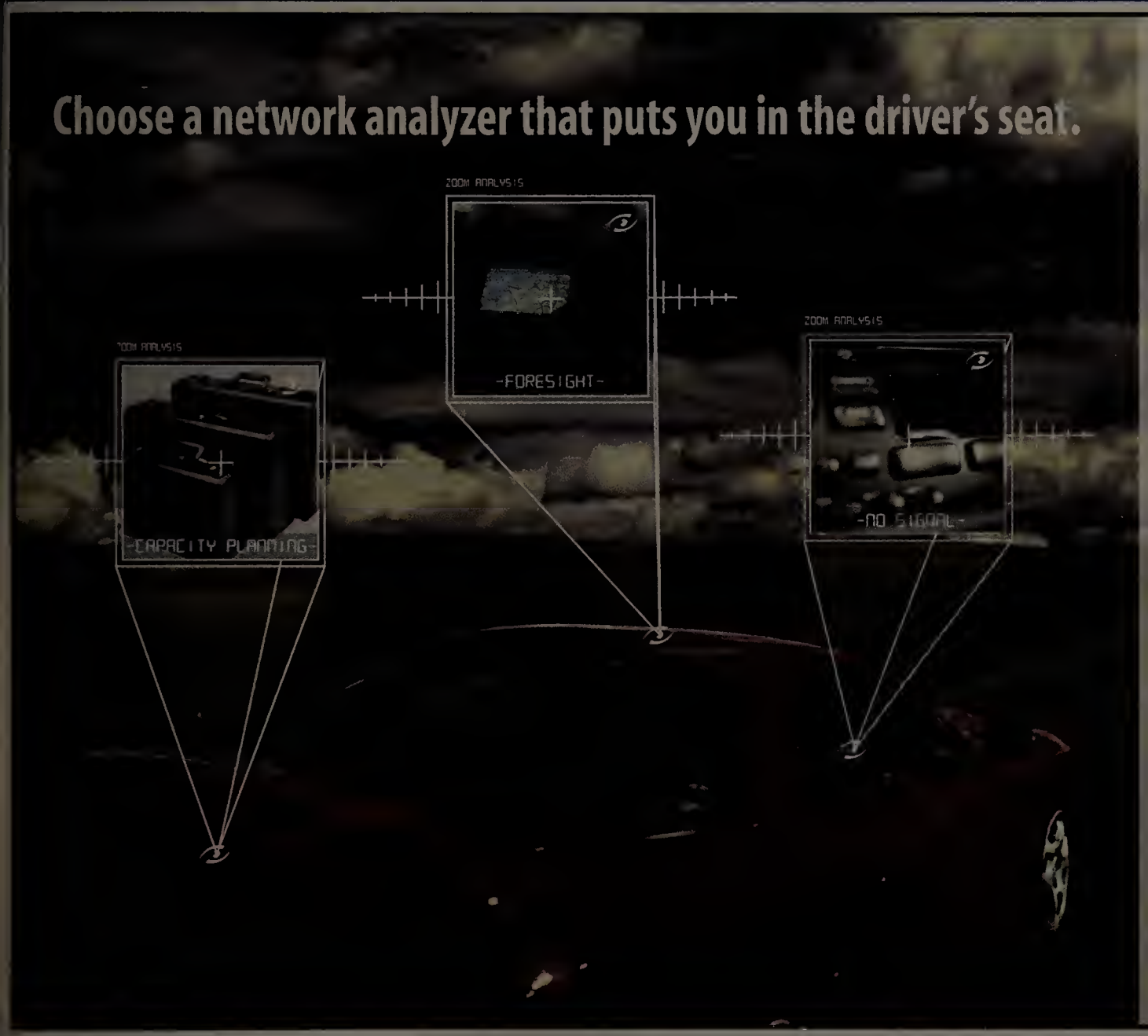
Climate Monitor $399

Heat
Humidity
Air Flow
Sound
Doors
Power
Camera

(512)257-1462 ITWatchdogs.com

WWW.SUITCASE.COM

Luggage, Fine Leather Goods, Gifts, and more!
Tumi, Hartmann, Andiamo, Samsonite, Cross
10% discount for Network World readers
Enter code NWW 2005



Choose a network analyzer that puts you in the driver's seat.

NETWORK INSTRUMENTS®

OBSERVER

How much does your network analyzer see?

Observer is the only fully distributed network analyzer built to monitor the entire network (LAN, 802.11a/b/g, Gigabit, WAN). Download your free Observer 10 evaluation today and see how Observer puts you in the driver's seat with more real-time statistics, more in-depth analysis and more network advantages than ever before. Choose Observer.

-CAPACITY PLANNING- Determine how much bandwidth your router will need based on historical usage patterns with Network Trending.

-FORESIGHT- Predict how network changes will affect your response times with "What-If" Modeling Analysis.

-NO SIGNAL- Find rogue access points, monitor access point load and scan wireless channels continuously with over 50 WLAN Expert Conditions.

US & Canada toll free 800.526.5958
fax 952.932.9545

UK & Europe +44 (0) 1959 569880

www.networkinstruments.com/analyze

dtSearch® Instantly Search Gigabytes of Text Across a PC, Network, Intranet or Internet

Publish Large Document Collections to the Web or to CD/DVD

- over two dozen indexed, unindexed, fielded & full-text search options
- highlights hits in HTML, XML, & PDF while displaying embedded links, formatting & images
- converts other file types (word processor, database, spreadsheet, email, ZIP, Unicode, etc.) to HTML for display with highlighted hits

"The most powerful document search tool on the market" –*Wired Magazine*

"Intuitive and austere ... a superb search tool" –*PC World*

"Blindingly fast" –*Computer Forensics: Incident Response Essentials*

"A powerful arsenal of search tools" –*The New York Times*

dtSearch "covers all data sources ... powerful Web-based engines" –*eWEEK*

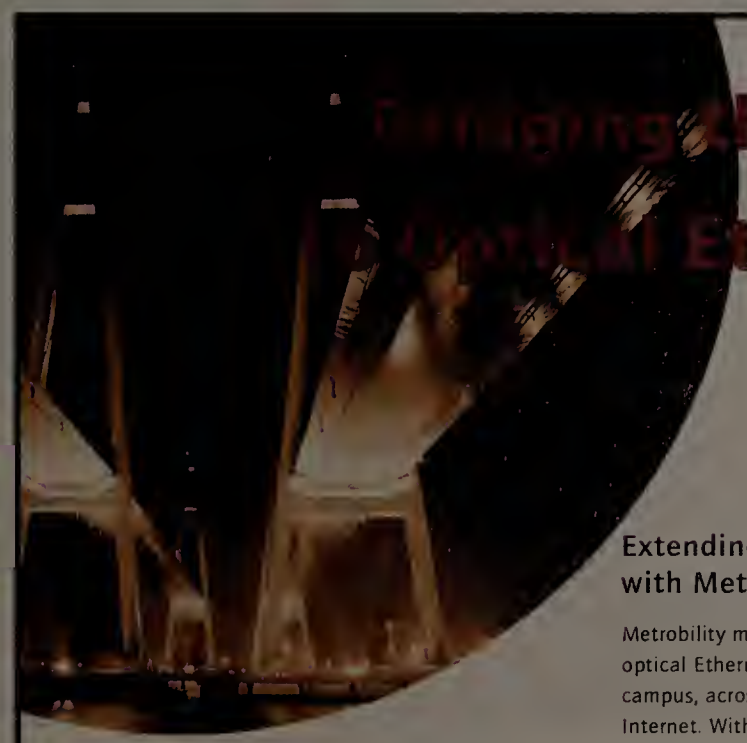
"Searches at blazing speeds" –*Computer Reseller News Test Center*

In the past two years, over half of the Fortune 15 purchased dtSearch *developer* or *network* licenses.

See www.dtsearch.com for:
- hundreds of developer case studies & reviews
- fully-functional evaluations

1-800-IT-FINDS
sales@dtsearch.com

The Smart Choice for Text Retrieval® since 1991



Bridging the Gap to Optical Ethernet

Extending the Enterprise LAN with Metro Ethernet Services

Metrobility makes it easy to deploy optical Ethernet services across the campus, across town, and across the Internet. With support for multimode, singlemode, and wavelength multiplexing even the most demanding requirements can be met.

Multi-level standards-based management and enhanced diagnostic capabilities mean staff training will be minimized and network reliability and performance are improved.

Find out how Metrobility can help you extend your LAN and maximize your infrastructure with optical Ethernet.

The E-Services NID
Intelligent, secure demarcation for Ethernet in the First Mile

See us at Networld+Interop
Booth 2117

METRObility optical systems

www.metrobility.com ph: 1.603.880.1833 toll-free 1.800.952.6227

Sales Offices

Carol Lasker, Associate Publisher/Vice President
Jane Weissman, Sales Operations Manager
Internet: clasker, jweissman@nww.com
(508) 460-3333/FAX: (508) 460-1237

New York/New Jersey
Tom Davis, Associate Publisher, Eastern Region
Elisa Della Rocco, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: tdavis, elisas, ajoseph@nww.com
(201) 634-2300/FAX: (201) 634-9286

Northeast
Elisa Della Rocco, Regional Account Director
Internet: elisas@nww.com
(508) 460-3333/FAX: (508) 460-1237

Mid-Atlantic
Jacqui DiBianca, Regional Account Director
Renee Wise, Sales Assistant
Internet: jdibian, rwise@nww.com
(610) 971-1530/FAX: (610) 975-0837

Midwest/Central
Eric Danetz, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: edanetz, ajoseph@nww.com
(201) 634-2314/FAX: (201) 712-9786

Southeast
Don Seay, Regional Account Director
Renee Wise, Sales Assistant
Internet: dseay, rwise@nww.com
(404) 504-6225/FAX: (404) 504-6212

Northern California/Northwest
Sandra Kupiec, Associate Publisher, Western Region
Karen Wilde, Regional Account Director
Courtney Cochrane, Regional Account Director
Vanessa Tormey, Regional Account Manager
Teri Marsh, Sales Assistant
Jennifer Hallett, Sales Assistant
Internet: skupiec, kwilde, ccochrane, vtormey, tmarsh, jhallett@nww.com
(510) 768-2800/FAX: (510) 768-2801

Southwest/Rockies
Becky Bogart Randell, Regional Account Director
Internet: brandell@nww.com
(949) 250-3006/FAX: (949) 833-2857

Online/Integrated Solutions
Kevin Normandeau, Vice President, Online
Susan Cardoza, National Sales Director, Integrated Solutions
Scott Buckler, Director of Integrated Solutions
Stephanie Gutierrez, Online Acct. Manager, Integrated Solutions
Michael Hiatt, Director of Integrated Solutions
James Kalbach, Director of Integrated Solutions
Debbie Lovell, Online Account Manager, Integrated Solutions
Kate Zinn, Director of Integrated Solutions
Denise Landry, Sales Coordinator
Lisa Thompson, Sales Coordinator
Internet: knormandeau, scardoza, sbuckler, sgutierrez, mhiatt, jkalbach, dlovell, kzinn, dlandry, lthompson@nww.com
(508) 460-3333/FAX: (508) 861-0467

MARKETPLACE/EMERGING MARKETS
Donna Pomponi, Director of Emerging Markets
Enku Gubaie, Manager of Marketplace/Emerging Markets
Caitlin Horgan, Manager of Marketplace/Emerging Markets
Jennifer Moberg, Manager of Marketplace/Emerging Markets
Chris Gibney, Sales Operations Coordinator
Internet: dpomponi, egubaie, chorgan, jmoberg, cgibney@nww.com
(508) 460-3333/FAX: (508) 460-1192

Network World, Inc.

118 Turnpike Road, Southborough, MA 01772
Phone: (508) 460-3333

TO SEND E-MAIL TO NWW STAFF
firstname_lastname@nww.com

Evilee Thibeault, CEO/Publisher
John Gallant, President/Editorial Director
W. Michael Draper, Chief Operating Officer
Eleni Brisbois, Administrative Planning Manager

FINANCE
Mary Fanning, Vice President Finance
Paul Mercer, Finance Manager
Betty Amaro-White, Event Finance Manager

HUMAN RESOURCES
Eric Cormier, Sr. Human Resources Generalist

MARKETING
Terry Ann Croci, Sr. Director of Customer Experience
Nancy Sarlan, Corporate Marketing Communications Mgr.
Barbara Sullivan, Senior Research Analyst
Judy Schultz, Marketing Design Manager
Cindy Panzera, Marketing Designer

PRODUCTION SERVICES
Greg Morgan, Senior Director, Production Services
Karen Wallace, Senior Director, Advertising Operations
Mike Guerin, Manager of Production Technologies
Jami Thompson, Sr. Production Coordinator
Veronica Trotto, Online Operations Coordinator
Jane Wilbur, Online Ad Traffic Coordinator
Maro Eremyan, Advertising Coordinator
Christina Pankievich, Advertising Coordinator

CIRCULATION
Richard Priante, Senior Director of Circulation
Bobbie Cruse, Subscriptions Manager
Mary McIntire, Sr. Circulation Marketing Manager

RESEARCH
Ann MacKay, Research Director

DISTRIBUTION
Bob Wescott, Distribution Manager/(508) 879-0700

IDG LIST RENTAL SERVICES
Amy Bonner, Account Executive
P.O. Box 9151, Framingham, MA 01701-9151
Toll free: (800) 434-5478 ext. 6026/Direct:(508) 370-0826
Fax: (508) 370-0020

SEMINARS, EVENTS AND IDG EXECUTIVE FORUMS
Neal Silverman, Vice President of Events & E. F.
Mike Garity, Director of Business Development
Michele Zarella, Director of Operations
Dale Fisher, Senior Event Planner
Jacqueline DiPerna, Event Coordinator
Karen Bornstein, Sales Operations Specialist
Danielle Bourke, Event Operations Coordinator
Andrea D'Amato, National Sales Director Events
Kristin Ballou-Cianci, Event Regional Account Director
Jennifer Sand, Regional Account Manager
Cedric Fellows, Regional Account Manager
Mark Hollister, Senior Director of Event Marketing
Debra Becker, Dir., Marketing & Audience Development
Sara Nieburg, Senior Marketing Manager
Dori Smith, Event Database Manager
Buster Paris, Marketing Specialist

ONLINE SERVICES
Kevin Normandeau, Vice President, Online
Dan Gallagher, Director of Audience Development, Online
Norm Olean, Director of Business Development, Online
Adam Gaffin, Executive Editor, Online
Melissa Shaw, Managing Editor, Online
Jason Meserve, Multimedia Editor
Sheryl Hodge, Sr. Online Copy Chief
Deborah Vozikis, Design Manager Online

CLIENT SERVICES
W. Michael Draper, Chief Operating Officer
Sharon Stearns, Director of Client Services
Leigh Gagin, Client Services Manager
Kristin Miles, Client Services Specialist

INFORMATION SYSTEMS/BUSINESS SERVICES
W. Michael Draper, Chief Operating Officer
Tom Kroon, Director of Systems Development
Anne Nickinello, Senior Systems Analyst
Puneet Narang, Manager of Database Technologies
William Zhang, Senior Software Engineer
Manav Seghal, Senior Software Engineer
Rocco Bortone, Director of Network IT
Peter Hebenstreit, Senior Network/Telecom Engineer
Brian Wood, Senior Systems Support Specialist
Frank Coelho, Senior Manager, Business Services
Mark Anderson, Business Services Supervisor
Linda Cavanagh, Business Services Administrator

IDG

Patrick J. McGovern, Chairman of the Board
Pat Kenealy, CEO

Network World is a publication of IDG, the world's largest publisher of computer related information and the leading global provider of information services on information technology. IDG publishes over 275 computer publications in 75 countries. Ninety million people read one or more IDG publications each month. *Network World* contributes to the IDG News Service, offering the latest on domestic and international computer news.

Editorial Index

A
Aastra 52
ADIC 25
AOL 6
Aruba Wireless Networks 22
AT&T 1, 35
Azul Systems 25

B
BMC Software 6
BT Infonet 35

C
Cisco 6, 10, 39
Colubris Networks 22

E
enKoo 17

F
FineGround 25
Force10 Networks 17

H
HP 61

I
IBM 6, 30

L
LapWorks 44
LifeSize Communications 20

M
Microsoft 9, 27

N
Nortel 8

O
Occam Networks 35

P
PSS Systems 29

Q
Qualsys 17

S
SAP 29
SMC Networks 17
Softricity 25
Spectralink 22
SpikeSource 29
Symantec 17

T
Trapeze Networks 22
TriCerat 25
Tritton Technologies 39

V
Vonage 35

Advertiser Index

Advertiser	Page #	URL
Adtran	21	www.adtran.com/rightprice
Avocent	4	www.avocent.com/control
Barracuda Networks	37	www.barracudanetworks.com/NECC
Cisco Systems	26	cisco.com/poweredby
Cisco Systems	27	cisco.com/go/cpnnow1
Communication Devices Inc	58	www.outofbandmanagement.com
Cyclades Corp	57	www.cyclades.com/nw
dtSearch Corp	59	www.dtsearch.com
EMC Corp	16	www.EMC.com/backup
Executive Software	40	www.diskeeper.com/nww9
Fluke Networks	7	www.flukenetworks.com/optiviewdemo
Foundry Networks	63	www.foundrynet.com/sx
*Hewlett Packard	45	www.hp.com/go/bladesmag52
*Hewlett Packard	45	hp.com/info/integrity
IBM Corp	31	ibm.com/middleware/resource
IBM Corp	32-33	ibm.com/information
IBM Corp	64	ibm.com/db2/swap
Intel Corp	18-19	intel.com/go/xeon
Ipswitch Inc	36	www.ipswitch.com
IT Watchdogs	58	ITWatchdogs.com
Layton Technology Inc	53	www.audtwizard.com
Linksys	38	www.linksys.com/SRX
Metrobility Optical Systems	59	www.metrobility.com
Microsoft Corp	2-3	microsoft.com/wssystem
Mirapoint Inc	24	mirapoint.com/done
MovinCool	58	www.movincool.com
Network Instruments LLC	56	www.networkTAPs.com/visibility
Network Instruments LLC	59	www.networkinstruments.com/analyze
Novell Inc	9, 11, 13, 15	novell.com
Oracle Corp	23	dell.com/database
Oracle Corp	51	oracle.com/integration
Phonetics Inc	56	www.ims-4000.com
*Quantum Corp	34	DLTtape.com
Raritan Computer	54	www.The MotherofAllAlarmStorms.com
Recurrent Technologies, Inc	58	www.recurrent.com
Rose Electronics	56	www.rose.com
Server Technology Inc	58	www.servertech.com
VeriSign Inc	42-43	www.VeriSign.com
Xerox Corp	28	xerox.com/office

Network World Fusion - www.nwfusion.com

3Com	Network Associates
ADIC	Nokia
Airespace	Nortel Networks
Allot Communications	Oracle Corporation
Avaya	PatchLink Corporation
BMC	Program Deliverables
Broadcom Corporation	Qwest Communications
CDW	RADWARE
Ceonex, Inc.	Redline Networks
Chantry Networks	Remedy
Cisco Systems, Inc.	Riverbed Technology
Computer Associates	RSA Security Inc.
DuPont	SBC
EMC Corp	Schmidt's LOGIN GmbH
Engenio	Sprint
Finisar Corp	SSH Communications
Groundwork	Statscout Pty Ltd
HP	Texas Instruments
IBM	Trend Micro
Imprivata	TrendsMedia Inc.
Intel Corporation	Tripp Lite
IronPort Systems	VeriSign Inc
Juniper Networks Inc	Verizon Wireless Broadband
Lucent Technologies	Webroot
Meru	Xerox
Microsoft Corporation	

These indexes are provided as a reader service. Although every effort has been made to make them as complete as possible, the publisher does not assume liability for errors or omissions.

*Indicates Regional Demographic

Network World, 118 Turnpike Road, Southborough, MA 01772-9108, (508) 460-3333.

Periodicals postage paid at Southborough, Mass., and additional mailing offices. Posted under Canadian International Publication agreement #40063800. Network World (ISSN 0887-7661) is published weekly, except for a single combined issue for the last week in December and the first week in January by Network World, Inc., 118 Turnpike Road, Southborough, MA 01772-9108.

Network World is distributed free of charge in the U.S. to qualified management or professionals.

To apply for a free subscription, go to www.subscribenw.com or write Network World at the address below. No subscriptions accepted without complete identification of subscriber's name, job function, company or organization. Based on the information supplied, the publisher reserves the right to reject non-qualified requests. Subscriptions: 1-508-490-6444.

Nonqualified subscribers: $5.00 a copy; U.S. - $129 a year; Canada - $160.50 (including 7% GST, GST#126659952); Central & South America $150 a year (surface mail); Europe - $205 a year (surface mail), all other countries - $300 a year (airmail service). Four weeks notice is required for change of address. Allow six weeks for new subscription service to begin. Please include mailing label from front cover of the publication.

Network World can be purchased on 35mm microfilm through University Microfilm Int., Periodical Entry Dept., 300 Zebb Road, Ann Arbor, Mich. 48106.

PHOTOCOPYRIGHTS: Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by Network World, Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $4.00 per copy of the article, plus 50 cents per page is paid to Copyright Clearance Center, 27 Congress Street, Salem, Mass. 01970.

POSTMASTER: Send Change of Address to **Network World**, P.O. Box 3090, Northbrook, IL 60065. Canadian Postmaster: Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A7C9.

Copyright 2005 by Network World, Inc. All rights reserved. Reproduction of material appearing in Network World is forbidden without written permission.

Reprints (minimum 500 copies) and permission to reprint may be purchased from Reprint Management Services at (717) 399-1900 x129 or mshober@reprintbuyer.com.

USPS735-730

HP adds dual-core processor to Opteron blades

■ BY ROBERT MCMILLAN

Only days before the launch of Advanced Micro Devices' first dual-core Opteron microprocessor, HP began taking orders for a four-processor blade system that will use the chips.

HP's new system, the ProLiant BL45p, will ship with a 2-GHz dual-core processor called the Opteron 875, according to HP's Web site. HP plans to announce the BL45p this week, with shipments beginning 20 to 30 days after the announcement, a company spokeswoman confirmed.

AMD and chip rival Intel have been racing to be first to ship processors with two computational engines, called cores, on a single processor. AMD is expected to launch its processors at an April 21 event in New York.

The new HP blade is based on a similar design to HP's four-way Xeon, the BL40p, but with AMD's dual-core processors, it is the first blade server from a major vendor to have so many processing engines. The dual-core Opterons are designed to use the same amount of power as their single-core predecessors, and AMD has had to reduce the clock speed of the processors to 2GHz to add the second processing engine without driving up the chip's power requirements. AMD's single-core Opterons have a maximum clock speed of 2.6 GHz.

With the launch of the BL45p, HP's Opteron blade line will be as broad as its Xeon offerings. By year-end, the company intends to also begin shipping its first blade system based on Intel's Itanium 2 processor, company officials have said. Analysts say that this third line of blade products likely will be based on Intel's upcoming dual-core Itanium processor, code-named Montecito.

Blades have emerged as an alternative to rack-mounted servers in recent years. Smaller than rack servers, they slide side-by-side into a special chassis, which lets them share resources such as network cables, power and cooling. Though the market initially was slow to adopt blades, they have become more popular of late. Gartner estimates that about 290,000 blades were shipped in 2004. It expects that number to nearly double in 2005.

HP is going through the process of making all of its server products available in this new form, says John Enck, a Gartner analyst. "They're simply trying to duplicate . . . all their servers in the blade environment," he says. "They're the only one of the vendors that is supporting Xeon and Opteron."

Part of the reason for HP's blade focus is that with the complex engineering work that goes into the blade chassis and management software, there is still plenty of room for HP to create products that are unique, says Ann Livermore, the executive vice president of HP's Technology Solutions Group.

Meanwhile, Dell has no plans to begin shipping Opteron systems, and while IBM has said that it intends to ship an Opteron blade, it has not yet revealed any details on this product.

A dual-processor version of the BL45p was listed for $3,000 on HP's Web site. Additional processors were listed as $1,000 each, the site showed.

McMillan is a correspondent with the IDG News Service.

Bio-IT World
CONFERENCE+EXPO
Technologies Driving Discovery, Development and Clinical Trials

MAY 17 – 19, 2005
BOSTON, MA
HYNES CONVENTION CENTER

Tuesday, May 17
Tim Berners-Lee
World Wide Web Consortium
Introduction by Life Science Insights

Wednesday, May 18
Lawrence J. Lesko PhD, FCP
Office of Clinical Pharmacology and Biopharmaceutics, CDER/FDA

Thursday, May 19
J. Craig Venter, PhD
The J. Craig Venter Institute

Be part of the only major event that focuses on the integration of technologies for research, drug discovery and clinical trials.

ADVANCES IN GENOMIC MEDICINE
FEATURED SPEAKER:
Nicholas C. Dracopoli, PhD
VP, Clinical Discovery Technologies, Genomics, Bristol-Myers Squibb

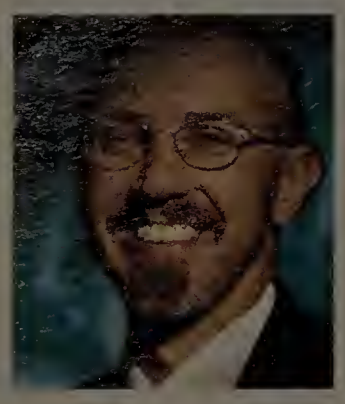
IT SOLUTIONS FOR DRUG DISCOVERY
FEATURED SPEAKER:
Steve Walker
CIO
UK Biobank, UK
Sponsored by hp invent

ECLINICAL TRIALS & RESEARCH
FEATURED SPEAKER:
Sylva H. Collins, PhD
VP, Advanced Clinical Systems
Novartis Pharmaceuticals
Sponsored by CRF Connected for Health

GOLD SPONSOR: EMC² where information lives; IBM
SILVER SPONSORS: Waters; FUJITSU; EXPEDATA; hp invent
ASSOCIATION PARTNERS: iSCB; NCGR; Bioinformatics.Org
FLAGSHIP MEDIA SPONSOR: Bio-IT World
MEDIA SPONSORS: Cell; Science AAAS; NetworkWorld; Pharmaceutical Business Strategies; Biotechnology Focus; LinuxWorld Magazine; nature methods; nature reviews; Sigma Xi American Scientist; D&MD Publications; PharmaVOICE; LAB ON A CHIP; GRID today; DSstar; biocompare www.biocompare.com; Technology Review; HPC; nature biotechnology

Register Today!
www.bio-itworldexpo.com

BackSpin Mark Gibbs



Forced to upgrade without complaint

A recent survey by AssetMetrix showed that less than 24% of more than 136,000 PCs in 251 North American corporations had been "upgraded" to Windows XP Service Pack 2.

I find it interesting that pretty much everyone refers to SP2 as an "upgrade." Microsoft's preferred spin is that SP2 provides a number of enhancements for Internet Explorer along with an Outlook Express privacy update, an attachment manager, the Windows Security Center, a Windows Firewall update, an enhancement to Automatic Updates, improved wireless support, a new version of Windows Media Player and a DirectX update.

None of these is critical. Some of the items are just fluff. Consider the Windows Media Player: There is nothing remotely critical about a new version of this utility. On the other hand bug fixes, particularly where security is involved, are truly critical.

SP2 isn't so much an upgrade as a bulk bug fix. So how many bug fixes are involved? Just take a look at the Microsoft Knowledgebase article "List of fixes included in Windows XP Service Pack 2" (see www.nwfusion.com, DocFinder: 6750).

This list details 830 bug fixes, of which 151 are labeled as applying to the base operating system and COM+, 76 involve the Windows shell, 75 concern management and administration, 19 are program compatibility issues, 73 are for security, and a staggering 161 deal with network problems.

These fixes are on top of the 321 that were included in the previous "upgrade," called Service Pack 1. We have a total of 1,151 bug fixes since XP was released in October 2001.

The AssetMetrix study also found that 41% of companies using XP have actively avoided upgrading to SP2, while a measly 8% actively accepted it. The remaining 51% of companies apparently "showed no direction or policy toward SP2 and may find themselves having support issues by allowing multiple editions of Windows XP to exist in their infrastructure."

These statistics are interesting because Microsoft last August, in response to customer demands (another way of saying "howls of protest"), allowed customers to optionally suspend the delivery of SP2 by Microsoft's Automatic Update service. That suspension expired on April 12.

AssetMetrix pointed out that "Companies choosing not to deploy SP2 will be faced with a host of potential issues, including possible incompatibilities with future products such as Internet Explorer 7, or a potential support gap when Microsoft support for Windows XP Service Pack 1 is withdrawn in September 2006."

Four out of 10 organizations are avoiding the installation of XP2 despite the risks involved. The only reason I can think of is because of the testing required. This obviously is a big issue for large IT shops because it takes a huge amount of effort to find where the upgrade is going to break your systems.

Given the size of SP2, it's hard to figure out how much time organizations would need to test it. Is the eight months Microsoft allowed adequate in real-world IT, given the several million other pressing matters of equal or greater importance?

The big question is why doesn't Microsoft slim down the Service Packs? Why doesn't it identify the bug fixes that apply to the security and reliability of the core operating system and services of XP, and make those required if we're to receive further fixes? It should be a matter of choice. Organizations that don't want to update their systems could choose to stall out at some patch level and become unsupportable by Microsoft.

The answer is marketing. By requiring these massive service packs of critical bug fixes, combined with self-serving product enhancements, Microsoft reinforces its stranglehold on the market. Why don't I hear more complaining?

Sound off to backspin@gibbs.com. And there's always Gearblog (www.nwfusion.com/weblogs/gearblog).

'NetBuzz News, insights, opinions and oddities

By Paul McNamara

Stealing at Internet2 speed

Toss the keys to your Porsche at any college kid . . . and don't act surprised when the cops clock him doing a buck-twenty-something out on the interstate.

University administrators and IT executives are relearning this age-old lesson in the wake of last week's embarrassing revelation that hundreds of students nationwide — at Harvard, MIT and UC Berkeley, among others — are being sued for using their school-granted access to the super-speedy Internet2 to illegally swap music and movies.

The students remain unidentified as of this writing, and, of course, the plaintiffs have yet to substantiate their allegations in a court of law. But presuming the civil complaints stick, it should prove enlightening to see how university officials deal with this latest escalation in the ongoing war between intellectual property owners and those who have a greater appetite for free stuff than they do respect for the law.

Escalation is the right word here because Internet2 raises the theft-loss stakes considerably for the recording and movie industries. A song that might take 5 minutes to download over a cable or DSL connection on the Internet requires a mere 20 seconds over Internet2. A DVD-quality movie reportedly can be snatched in less than 5 minutes, as opposed to well over an hour via your garden-variety broadband Internet connection.

Little wonder that the 405 students being sued for trafficking in stolen music had harvested and were offering to "share" an average of 2,300 songs apiece, according to the Recording Industry Association of America. The Motion Picture Association of America last week was set to weigh in late with its own lawsuits.

The apologists for music and video thievery will argue that this episode offers more evidence of the futility of protecting old-world intellectual property rights in an era in which technological innovation reigns supreme. Of course, the apologists can afford to make such a case because it isn't their property being stolen.

And while critics lambaste the entertainment industries for defending their property through lawsuits instead of embracing new business models, the recording and film executives need to live in the real world — as do the college administrators and IT officials whose participation in Internet2 has been sullied.

So how will academia respond? If recent precedent is any guide, you can expect the reactions to run the gamut.

As you may recall, a number of the nation's elite business schools recently dealt with a security breach that found would-be students exploiting instructions found online to gain access to computer records about their applications. Some schools automatically rejected all those who peeked, while others were more lenient.

Harvard Business School was among those taking a hard-line. "Our mission is to educate principled leaders who make a difference in the world," said the dean when the institution announced it would no longer consider admitting the 119 men and women who stole a look at their application status. "To achieve that, a person must have many skills and qualities, including the highest standards of integrity, sound judgment and a strong moral compass. Those who have hacked into this Web site have failed to pass that test."

As for currently enrolled students who use school property to steal music and videos? . . . We'll have to wait and see.

Personally, I had no problem with the universities that summarily bid farewell to those applicants who just couldn't wait for that letter to arrive in the mailbox.

As for the 'Net abusers, every university has an acceptable use policy and you can be certain not one condones theft. And not even a college kid can plead ignorance at this point.

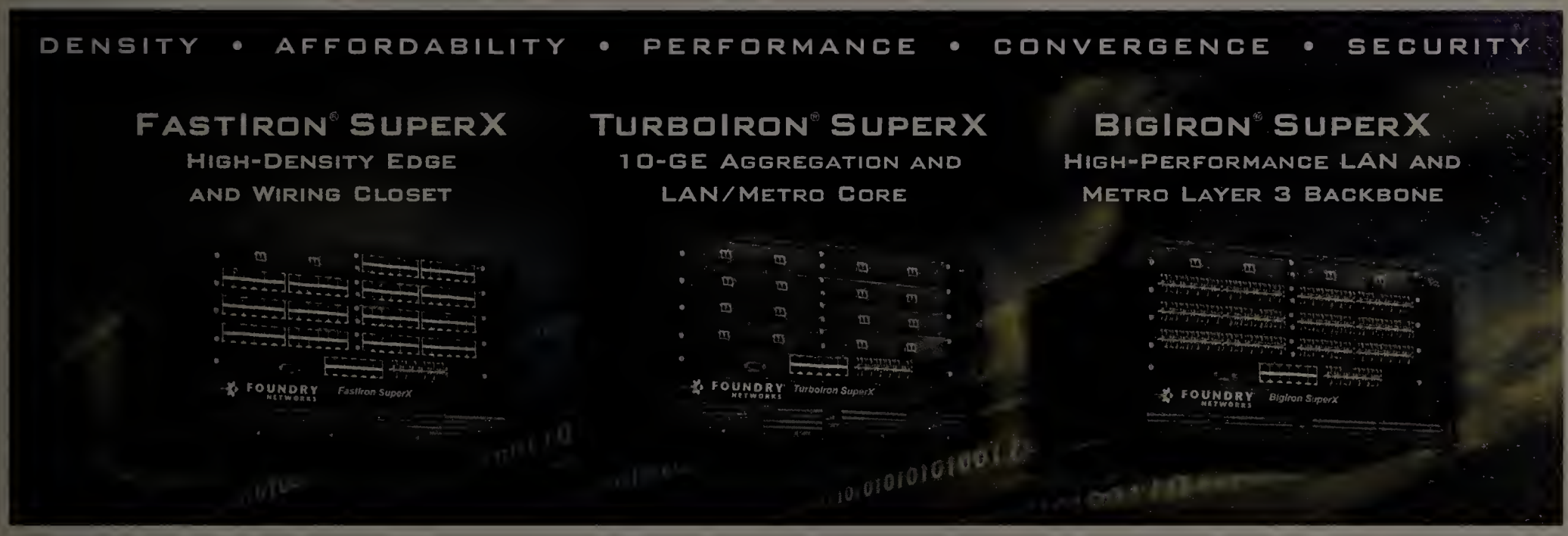
So does expulsion seem too harsh?

Maybe, but it also seems richly deserved.

Need to tell me again why the RIAA is evil and music-swapping ain't stealing? The address is buzz@nww.com.

SuperX™ 10-GE Switch Family

A Unified Architecture for Enterprise and Service Provider LAN and Metro Infrastructures



With the performance you expect from Foundry—now comes the price, flexibility, and density breakthrough you've been waiting for. The new SuperX family of Layer 2/3 modular switches provides the industry's highest Gigabit Ethernet and 10-GE density per rack and the lowest 10-GE price per port in a modular switch. The SuperX family delivers an extensive feature set, standards-based Power-over-Ethernet, support for full Layer 3 (including OSPF and BGP4), and wire-speed 10-GE solutions. From the enterprise to the service provider environment: SuperX is the right choice!

FastIron SuperX

- Edge & wiring closet switch
- Extensive QoS and security features
- Ease of upgrade to PoE

TurboIron SuperX

- 10-GE aggregation and core switch
- Pre-configured with 16 10-GE ports per switch
- Industry leading price of less than $2,500/10-GE port

BigIron SuperX

- Enterprise and metro L3 backbone switch
- High-performance Layer 3 routing processor
- Up to 1 million routes and 200+ BGP peers

High Density

- Up to 204 Ports GE-SFP Mini-GBIC
- Up to 204 Ports 10/100/1000
- Up to 192 Ports 10/100/1000 PoE
- Up to 16 Ports 10-GE

High Performance

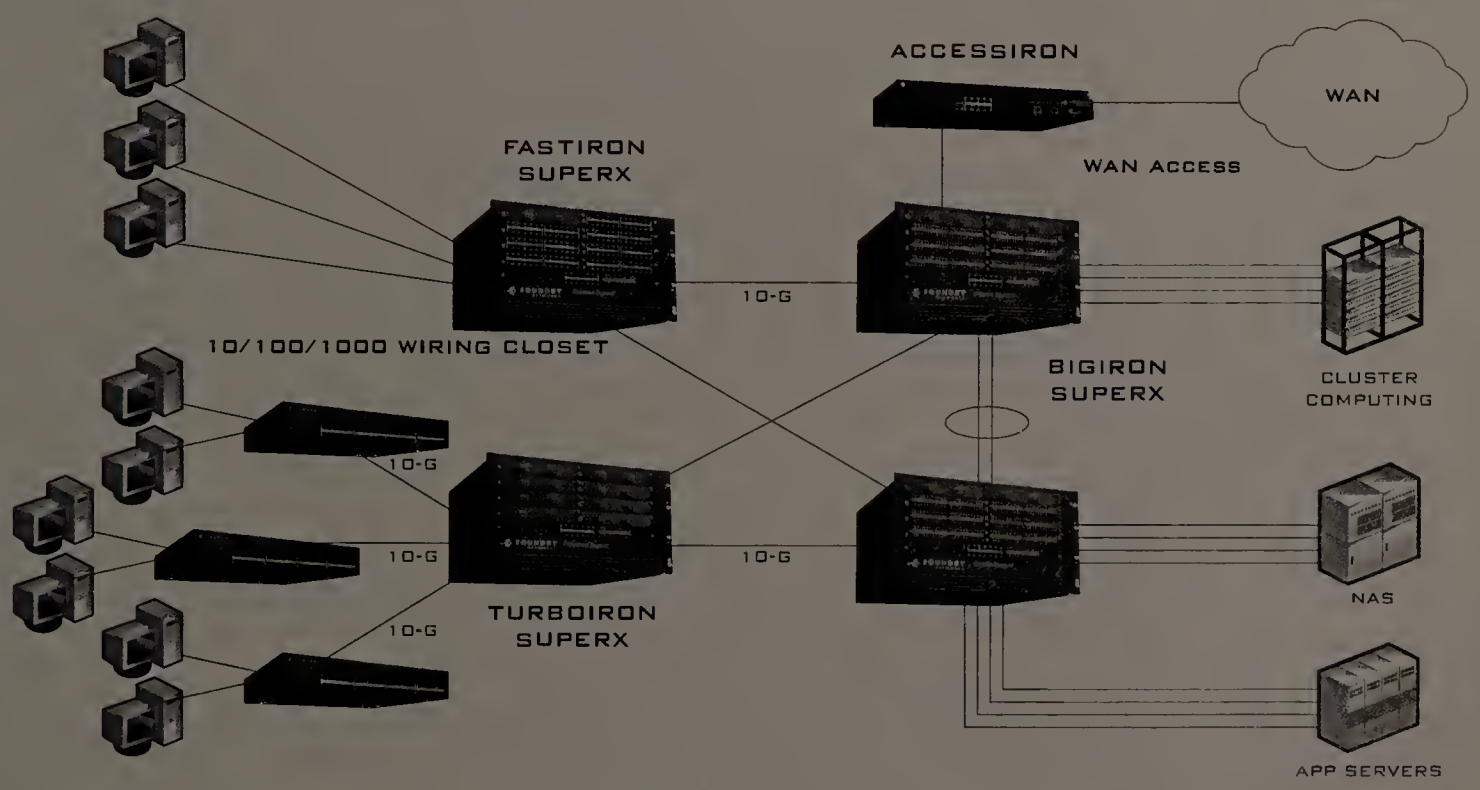
- Wire-Speed Every Port
- Up to 304 Mpps Throughput
- 510-Gbps Switching Capacity

Convergence Ready

- Standards-Based Power-over-Ethernet
- Purpose-Built for Data, Voice & Video
- Integrated Wired & Wireless Support

IronShield Security

- Wire-Speed ACLs & Rate Limiting
- Secure Shell, Secure Copy, SNMPv3
- DoS Attack Protection
- 802.1x & MAC Authentication with Dynamic Policy

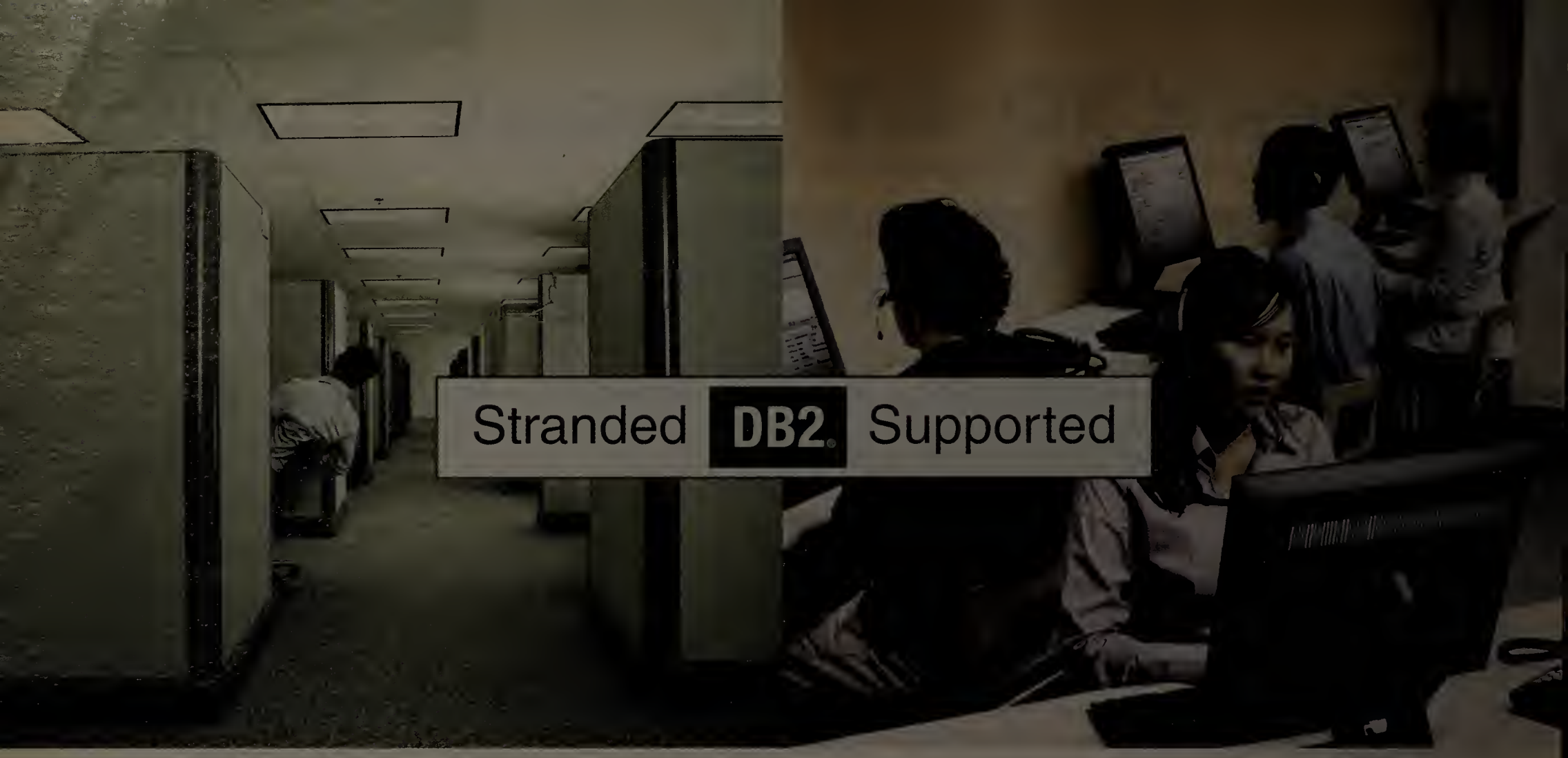


FOUNDRY® NETWORKS

The Power of Performance™

For more information please call:
US/Canada 1 888 TURBOLAN,
International +1 408.586.1700
or visit our website at www.foundrynet.com/sx

Foundry Networks, Inc. is a leading provider of high-performance Enterprise and Service Provider switching, routing and Web traffic management solutions including Layer 2/3 LAN switches, Layer 3 Backbone switches, Layer 4-7 Web switches, wireless LAN and access points, access routers and Metro routers.



DB2 WON'T ABANDON YOU.

Perhaps you've heard: Oracle desupported Oracle Database 8i last year. Meaning potential headaches, higher cost or a complete migration to current versions of Oracle. Fortunately, IBM offers ongoing, around-the-clock service and support for DB2.

But that's not all. A Solitaire study has found that, on average, Oracle Database requires 25% more time to manage than DB2.[1] That's big.

And an ITG study showed overall costs for Oracle Database up to four times higher than DB2.[2] The Transaction Processing Performance Council results show that DB2 and eServer™ p5-595 are more than twice as scalable as Oracle Real Application Clusters, making them the overwhelming performance and scalability leader for TPC-C.[3] That's big, too.

No wonder DB2 is regarded as the leading database built on and optimized for Linux,® UNIX® and Windows.® Like other IBM database engine products such as Informix® and Cloudscape,™ DB2 is part of an innovative family of information management middleware that integrates, and can actually add insight to your data.

It's also built to take full advantage of your existing heterogeneous and open environments, and is built to enable true grid computing.

Why not move up to middleware that makes sense? Now you can get IBM DB2 Universal Database or Informix by taking advantage of our extremely compelling trade-up program. Visit **ibm.com**/db2/swap today to find out if you qualify.

IBM

ON DEMAND BUSINESS™

IBM, the IBM logo, DB2, eServer, Informix, Cloudscape and the On Demand logo are trademarks or registered trademarks of International Business Machines Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. UNIX is a registered trademark of The Open Group in the United States and/or other countries. Other company, product and service names may be trademarks or service marks of others. © 2005 IBM Corporation. All rights reserved. [1]"DB2 Performance on IBM Server® pSeries and xSeries," Solitaire Interglobal Ltd., 2003; based on Oracle Database 9i. [2]"IBM Solutions for PeopleSoft Deployment in Mid-sized Businesses Quantifying the New Cost/Benefit Equation," July 2003, International Technology Group, Los Altos, California. [3]All referenced results are current as of 12/14/04. DB2 UDB v8.2 on IBM eServer p5 595 (64-way POWER5 1.9 GHz) and AIX 5.3L: 3,210,540 tpmC @ $5.19/tpmC available: May 15, 2005, vs. Oracle RAC 10g on HP Integrity rx5670 Cluster 64P (16 x 4-way Intel Itanium2 6M 1.5GHz): 1,184,893 tpmC @ $5.52/tpmC available: April 30, 2004. TPC Benchmark, TPC-C, tpmC are trademarks of the Transaction Processing Performance Council. For further TPC-related information, please see http://www.tpc.org/